Appendix 2 to

Sixth Amendment of

Master Services Agreement

DIR-ESS-MSI-407
April 20, 2020

Exhibit 2.1 Statement of Work   Page 1

State of Texas
Department of Information Resources

Exhibit 2.1
Statement of Work

Multi-Sourcing Services Integrator

DIR-ESS-MSI-407

April 20, 2020

Exhibit 2.1 Statement of Work   Page 2

Change Log			
CCR/CN	Amendment	Date	Description
CCR-000291	Amendment 1	3/31/2018	• Updated Section 3.9.4.1.1 to remove reference to Appendix F related to APM services.

CCR-000386	Amendment 6	4/20/2020	• Global edit throughout the document: replaced "DIR Shared Services" with "DIR Shared Technology Services".
			• Section 1.2 Operating Model: updated language to subsection 3 (Business Management) to clarify scope adjustments
			• Section 1.3.1.2 MSI Shared Services Systems: updated language to clarify scope for Customer Relationship Management Systems
			• Section 2.6.5 Solutioning: removed requirement for MSI responsibility for outreach solutioning leadership
			• Section 3.1.4 Management of Incidents: updated language to clarify MSI responsibilities
			• Section 3.3 Information Security Management:
			  ▪ removed requirements in subsections 3.3.1 through 3.3.4 to reflect scope transferred to Security Operations SCP,
			  ▪ moved requirements for MSI systems to Section 7.11 Equipment and Software Maintenance and Section 7.12 Software Support
			• Section 3.5.3 Request Management Operations for All Service Requests: updated language to clarify requirement.
			• Section 3.5.4 Request Management Operations the Successful Respondent Owns: updated language to clarify requirements.
			• Section 3.5.5 Request for Solution (RFS): updated language to reflect emphasis of ROM process requirement and removal of cross-SCP leadership responsibilities
			• Section 4.4.5.3: Removed optimization requirement
			• Section 4.4.6 Market Price Comparison: removed requirement; section intentionally left blank
			• Section 4.5 Customer Relationship Management: updated language to include Customer Relationship Management scope for overall account management, surveys, operational management, project management, and demand management.
			• Section 4.10 Strategy Management: updated subsection 4.10.1 Technology Planning to reflect updated requirements in support of Technology Solution Services SCP
			• Section 5.1 Enterprise Event Management: added language to reflect that this is an optional capability

Exhibit 2.1 Statement of Work   Page 3

Change Log			
CCR/CN	Amendment	Date	Description
			• Section 7.1.1.6: updated Chief Technology Officer role definition and added Customer Relationship Management personnel • Section 7.8 (4): updated to clarify requirement • Section 7.11 Equipment and Software Maintenance: updated to reflect MSI systems requirements transferred from Section 3.3 Information Security • Section 7.12 Software Support: updated to reflect MSI systems requirements transferred from Section 3.3 Information Security

Exhibit 2.1 Statement of Work   Page 4

Table of Contents

Exhibit 2.1 Statement of Work   Page 6

1 INTRODUCTION

The following documents comprise the entire Statement of Work (SOW) for the Multi-sourcing Services Integrator (MSI) Request for Offer (RFO):

1. Exhibit 2.1 – Multi-sourcing Services Integrator Statement of Work
2. Exhibit 2.2 – Termination Assistance Services
3. Exhibit 2.3 – IT Service Management Continuity
4. Exhibit 4.2 – Responsibility Matrix

The Successful Respondent shall follow the instructions contained within these and all other RFO and Master Service Agreement (MSA) documents, including all Exhibits.

1.1 Overview

The Successful Respondent shall provide a solution that supports all business processes described in this SOW in accordance with **Exhibit 4.2 Responsibility Matrix**. All Services, unless otherwise specifically stated, are included in the Charges.

The Successful Respondent shall be responsive to the current and future requirements of the Department of Information Resources (DIR) and DIR Customers by proactively anticipating needs and adjusting Services accordingly within the Charges. Requirements for New Services will be handled in accordance with **Section 11.5** of the Master Services Agreement (MSA) and the Successful Respondent shall assess the impact of these requirements on DIR's and DIR Customers' operating environments and supported applications in accordance with the terms of the MSA.

This SOW sets forth the Services that the Successful Respondent shall provide, as of the Commencement Date unless otherwise specified, for all Services that affect multiple Service Components.

The Successful Respondent shall provide Charges inclusive of all activities required to provide the Services set forth in this SOW, including project-related support activities.

This scope of work defines requirements the Successful Respondent must meet to achieve the objectives of this procurement.

Exhibit 2.1 Statement of Work
Page 7

1.2	Operating Model

DIR has defined an operating model aimed at achieving the overall program objectives through leveraging MSI capabilities. This model provides context for the MSI solution and outlines general responsibility boundaries between DIR, MSI and the Service Component Providers (SCPs).

As the overall service owner, DIR operates a sourcing management and governance organization that performs customer relationship leadership, service and sourcing strategy, service portfolio management, and contract and financial management roles.

The Successful Respondent shall provide common, cross-functional capabilities organized into four (4) sub-domains: Marketplace, Service Management, Business Management, and Operations Management. The high-level capabilities within each sub-domain are outlined below with the specific requirements described throughout this document.
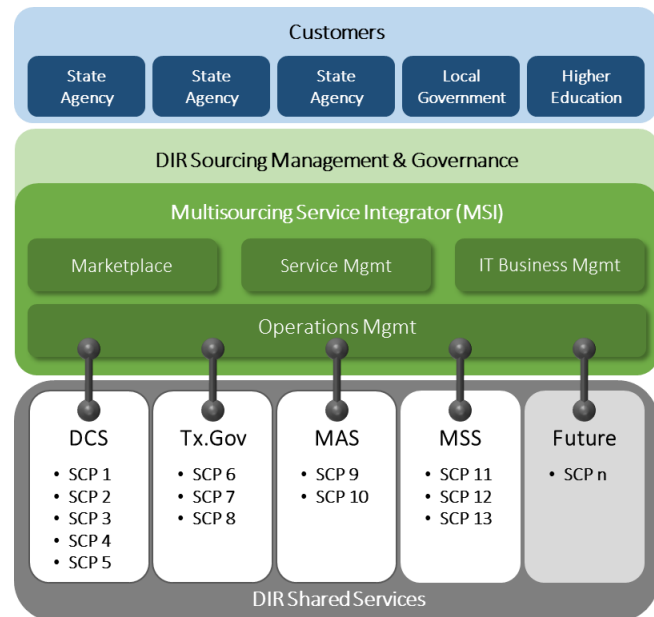
Figure 1

1. **Marketplace**

   a. Accessible service catalog with mobile access to order, approve, and view performance with near real time consumption analytics.

   b. Consumerized services experience from order through payment with integrated digital and contact center capabilities.

   c. Self-provisioning with a comparison of Services and pricing by Service Provider and orchestration of direct cloud resource provisioning, including public cloud.

   d. Advanced service desk platform with automated agent, advanced remote control, and intuitive tools enabling constituent help desk and premier IT service desk operations.

   e. Portal enabling customer and supplier digital collaboration, including access to MSI Shared Services Systems, training, and Service Management Manual (SMM) process documentation.

2. **Service Management**

   a. Automated core ITIL functions, centralized communications and a single system of record to enhance quality and increase speed to value.

   b. Digitally enabled change management including Digital Change Advisory Boards (CABs) and the automation of low-risk frequently-executed changes initiated from the Service Catalog and pre-approved.

Exhibit 2.1 Statement of Work   Page 8

c. Automated identification and validation of Configuration Items (CIs) and analytic dashboards to speed investigation and response.

d. Responsive and proactive security operations management.

e. Reactive and analytics-driven proactive problem management.

3. Business Management

a. Cross-functional project administration and enterprise program management.

b. Performance analytics that improve services and processes with real-time workflow data to provide visibility of projects and tasks.

c. Financial consolidation and transparency to generate supplier statements and customer chargeback, gain visibility into spending, connect costs to service usage, and align investment to business goals.

d. Customer relationship management providing the primary interface to DIR Customers for required aspects of DIR Shared Technology Services from operations, projects, to demand planning.

e. Enterprise customer relationship management through metrics and data analytics that provide operational intelligence in assisting customers to make more informed consumption management decisions.

4. Operations Management

a. Automated data quality management enabling accurate Configuration Management Database (CMDB) and more efficient identification of issues and restoration of services.

b. Aggregation of events and automated responsive actions to increase service availability and operational agility.

c. Enablement of self-provisioning and workflow orchestration.

d. Integration of cloud services in the service catalog to initiate and manage cloud resource provisioning through a cloud resource orchestration system and collect and report cloud usage and billing in a dashboard like fashion.

The SCPs will leverage and integrate with the MSI-provided capabilities to deliver supply-side services. These capabilities include integration with the MSI-provided cross-functional processes and systems, execution of SCP services scope, services monitoring, and SCP-level data presentation required to support the broader DIR operational and financial transparency.

1.3   MSI Shared Services Systems and Processes

DIR requires the Successful Respondent to provide capabilities and perform several roles in support of the overall DIR Shared Technology Services enterprise capabilities including:

1. Platform – Provide and support a cross-functional platform (systems and processes) that may be leveraged by DIR and DIR Customers for both internal operations as well as management of Shared Services.

Exhibit 2.1 Statement of Work   Page 9

2. Operate – Perform an operational role by providing the resources and execution of required roles.

3. Manage – Provide the capabilities and perform a managerial role to direct, oversee and ensure performance of DIR Shared Technology Services.

1.3.1 MSI Shared Services Systems

The Successful Respondent shall provide and maintain the systems required to support the DIR Shared Technology Services enterprise capabilities as noted in Table 1: MSI Shared Services Systems. The common requirements for these MSI-provided systems are noted below and the unique system requirements are described in the respective capability sections throughout this document.

The Successful Respondent shall:

Operating Model Sub-Domain	DIR Shared Services Enterprise Capabilities	Role			
		Platform (Provide Systems and Processes)	Operate (Provide staffing and perform a role)	Manage (Oversee and ensure performance)	Govern (Approve policies, manage program-level decisions)
Marketplace	Collaboration	MSI	MSI	MSI	DIR
	Service Catalog Management	MSI	MSI	MSI	DIR
	Service Desk and Constituent Help Desk	MSI	MSI	MSI	DIR
	Communications	MSI	MSI	MSI	DIR
	Outreach and Growth	MSI	MSI, SCP	MSI	DIR
Service Management	Incident Management	MSI	MSI, SCP	MSI	DIR
	Problem Management	MSI	MSI, SCP	MSI	DIR
	Information Security Management	MSI	SCP, MSI	DIR	DIR
	Access Management	MSI	MSI, SCP	MSI	DIR
	Request Management and Fulfillment	MSI	MSI, SCP	MSI	DIR
	Change Management	MSI	MSI, SCP	MSI	DIR
	Asset Inventory and Management	MSI	MSI, SCP	MSI	DIR
	Software License Management	MSI	MSI, SCP	MSI	DIR
	Configuration Management	MSI	MSI, SCP, Customer	MSI	DIR
	IT Service Continuity Management	MSI	MSI, SCP, Customer	MSI	DIR
	Project and Program Management	MSI	MSI, SCP	MSI	DIR
	Release Management	MSI	SCP	SCP	DIR
Business Management	Operational Intelligence	MSI	MSI, SCP	MSI	DIR
	Service Level Management	MSI	MSI, SCP	MSI	DIR
	Availability Management	MSI	MSI, SCP	MSI	DIR
	IT Financial Management	MSI	MSI, SCP	MSI	DIR
	Customer Relationship Management	MSI	MSI, DIR	DIR	DIR
	Service Delivery Management	MSI	MSI	MSI	DIR
	Capacity Management	MSI	MSI, SCP	MSI	DIR
	Risk Management	MSI	MSI, DIR	DIR	DIR
	Service Portfolio Management	MSI	DIR, MSI, SCP	DIR	DIR
	Strategy Management	12 to 18 mos view: MSI Long-term strategy: DIR	12 to 18 mos view: MSI Long-term strategy: DIR	DIR	DIR
Operations Management	Enterprise Event Management	MSI	MSI, SCP	MSI	DIR
	Data Quality Management	MSI	MSI/SCP	MSI	DIR
	Workflow Orchestration	MSI/SCP	MSI/SCP	MSI	DIR
	Cloud Management	MSI/SCP	MSI/SCP	MSI	DIR

Table 1: MSI Shared Services Systems

1.3.1.1 Provide equipment and software that complies with TAC 202 and applicable Texas Government Code, including the appropriate use of encryption and authentication controls.

1.3.1.2 Provide the following Successful Respondent Shared Services Systems:

Table 2: MSI Shared Services Systems Requirements

Operating Model Sub-Domain	DIR Shared Technology Services Enterprise Capabilities	MSI Shared Services Systems
Marketplace	Collaboration	**Portal** – System used as the centralized destination point of access to all documentation, shared information, system links and broadcast communications pertaining to the delivery of the Services.
		Learning Management System (LMS) – System used to deliver, administer, track and report on the delivery of electronic educational training.
	Service Catalog Management	**Service Catalog System** – System allowing users to shop, request and view status of services through an intuitive, easy to use storefront.
	Service Desk and Constituent Help Desk	**Service Desk Systems** – Systems required to provide service desk services including telephony, Automated Call Distributor (ACD), Integrated Voice Response (IVR), speech analytics, quality assurance, workforce management, knowledge repository.
	Communications	N/A

Exhibit 2.1 Statement of Work

	Outreach and Growth	**Customer Relationship Management Systems (CRM)** – Systems required to provide an end-to-end view of the relationship with the prospective and current Customers; including the tracking of outreach plans, campaigns, growth pipeline and Customer relationship management.
Service Management	Incident Management	**Incident Management System** – System providing initiation, tracking, prioritization, automated routing, resolution and recording of Service Incidents.
	Problem Management	**Problem Management System** - System that provides the ability to track, monitor, prioritize investigations, capture RCA results, and initiate Corrective Actions associated with the DIR Shared Technology Services.
	Information Security Management	**Security Incident Management System –** System providing initiation, tracking, prioritization, automated routing, resolution, and recording of Service security Incidents.
		Security Clearance Management System – System providing tracking of security clearances for all DIR Shared Technology Services personnel.
	Access Management	**Request Management System** – System providing initiation, tracking, prioritization, automated routing, resolution/fulfillment, and recording of Service Requests.
	Request Management and Fulfillment	
	Change Management	**Change Management System** – System that provides workflow-based tools to automate the process of recording, assessing, scheduling, documenting, authorizing, tracking, and reporting on Changes.
	Asset Inventory and Management	**Asset Inventory and Management System (AIMS)** – System that can track and manage all Equipment, Software, and related IT services (e.g., circuits, hardware, software).
	Software License Management	**Software License Renewal System** – System that provides tracking of software information including keys, monitoring, and reporting the software renewal process to ensure compliance with all software agreements, including SCP and Successful Respondent agreements.
		Software License Compliance System – System which determines Commercial-off-the-Shelf (COTS) compliance position to ensure compliance with software agreements and reduce operating risk in the environment.
	Configuration Management	**Configuration Management System** – System which incorporates information from multiple databases and sources providing a single, federated source for configuration item details that are used in the provisioning, support and management of DIR Shared Technology Services.
		Application Portfolio Management System – System that supports an optional DIR Shared Service through a centralized approach to collect, analyze and describe the relationships between a DIR Customer's business applications thereby allowing them to make informed, prioritized decisions about investments in technology services that support their business needs.

Exhibit 2.1 Statement of Work   Page 11

	IT Service Continuity Management	**ITSCM System** – Disaster recovery planning system to assist in the DR planning, administration and maintenance in support of the DIR Shared Technology Services IT Services Continuity program.
	Project and Program Management	**Project and Program Management System –** System that will serve as the single source of project planning, management, and information for all DIR Shared Technology Services projects and programs.
	Release Management	**Release Management System** – System to provide a structured environment to manage traditional waterfall and Agile release management and distribution processes enabling high quality implementations.
Business Management	Operational Intelligence	**Operational Intelligence System** – System to fulfill the requirements for operational reporting, operational measures, Key Performance Indicators (KPIs), Contract Performance Incentives (CPIs) at an enterprise, Customer, and SCP level.
	Service Level Management	**Service Level Management System** – System that will serve as the collector, management system, and reporting system for performance data provided by the Successful Respondent and SCPs, including Service Level Improvement Plans and associated improvement progress.
	Availability Management	**Availability Management System** – System that will serve as the collector, management system, and reporting system for application and infrastructure availability data and actions.
	IT Financial Management	**IT Financial Management System –** System that provides supply-side invoice generation and customer-side chargeback processing and Texas.gov Transaction Revenue reporting. Serves as the single source of information regarding all IT Financial information for DIR Shared Technology Services.
	Customer Relationship Management	**Customer Relationship Management Systems** – Systems required to provide an end-to-end view of the relationship with the prospective and current Customers, including the tracking of outreach plans, campaigns, outreach pipeline and Customer relationship management.
	Service Delivery Management	N/A
	Capacity Management	**Capacity Management System** – System to compile aggregated capacity and utilization information.
	Risk Management	N/A
	Service Portfolio Management	N/A
	Strategy Management	N/A
Operations Management	Enterprise Event Management	**Enterprise Event Management System** – System that serves as the collector and correlation system for forwarded events provided by MSI and Service Component Providers.
	Data Quality Management	**Data Quality Management System** – Provides an integration platform allowing the configuration of workflow processes and interfaces to electronically collect data from multiple sources, normalize the data, analyze data integrity issues and reconcile the data to the CMDB.

Exhibit 2.1 Statement of Work   Page 12

	Workflow Orchestration	**Workflow Orchestration System** – Platform with process workflow automation to enable increased self-service, automated issue remediation, automated Service Request resolution, and digital governance.
	Cloud Management	**Cloud Management System** – Platform to enable automated public and private cloud workflow orchestration across the MSI, Service Component Providers and directly to Cloud Service Providers (CSPs).

1.3.1.3   Design, deploy, and maintain an integrated Shared Services System to enable efficient and effective operations, management and governance of DIR Shared Technology Services Enterprise Capabilities across all SCPs which, at a minimum:

    1.3.1.3.1   Provide SCP, DIR, and DIR Customer access to the Successful Respondent's Shared Services Systems, including all appropriate and required license access and/or interfaces.

    1.3.1.3.2   Limit access to the Successful Respondent's Shared Services Systems to the agreed levels (e.g., by DIR Customer, SCP) for the type of Authorized Users who require access to the Successful Respondent's Shared Services Systems.

    1.3.1.3.3   Grant DIR access to the Successful Respondent's Shared Services Systems and allow DIR to monitor and view on an ongoing basis.

    1.3.1.3.4   Provide Successful Respondent personnel, other SCP personnel, DIR, and DIR Customers with appropriate training in using the Successful Respondent's Shared Services Systems.

    1.3.1.3.5   Lead efforts to design and integrate the SCP systems to the Successful Respondent's Shared Services Systems.

    1.3.1.3.6   Lead design efforts and configure the Successful Respondent's Shared Services-side workflow and interface capabilities to enable SCPs to initiate fully automated workflow processing.

    1.3.1.3.7   Provide a secure DIR Shared Technology Services operating environment.

    1.3.1.3.8   Record detailed audit trail information of all activity that creates, changes, or deletes data and user access to all Successful Respondent Shared Services Systems that contain DIR and DIR Customer data.

    1.3.1.3.9   Provide single sign-on access from the Portal to all Successful Respondent-provided systems and SCP systems as determined by DIR.

    1.3.1.3.10 Provide a solution that is scalable to efficiently and routinely onboard new Customers, new services, and new SCPs, as required by DIR.

    1.3.1.3.11 Leverage technology to perform automated process controls to enable digital governance and ensure process adherence for enterprise processes (e.g., Request Management, Change Management, Configuration Management) across the Successful Respondent, SCPs, DIR, and DIR Customers.

    1.3.1.3.12 Provide the functionality, data, and security to support the processes as defined in the SMM and support the reports as defined in **Exhibit 3.4, Performance Analytics**.

Exhibit 2.1 Statement of Work   Page 13

1.3.1.4 Leverage technology to coordinate automated execution of Shared Services Enterprise Capabilities across DIR, DIR Customers, and SCPs so that all individual components that make up DIR Shared Technology Services are managed in an end-to-end manner with seamless service delivery to DIR Customers.

1.3.2 MSI Shared Services Processes

DIR bases its SCP and MSI practices on ITIL, a world-wide recognized best-practice framework for the management and delivery of IT services throughout their full life-cycle. DIR expects the Successful Respondent to provide and maintain processes based on the ITIL 2011 framework as appropriate to support the DIR Shared Technology Services Enterprise Capabilities as noted in Table 1: MSI Shared Services Systems under the role of Platform.

In support of all DIR Shared Technology Services Enterprise Capabilities processes, the Successful Respondent shall:

1.3.2.1 Facilitate and lead in the development and maintenance of integrated processes within the MSI Shared Services processes and with other SCPs to enable consistent execution of IT services seamlessly across all environments and among SCPs.

1.3.2.2 Integrate processes with the supporting processes and functions of DIR, DIR Customers, and SCPs, with and where the processes and operations interact or have dependencies.

1.3.2.3 Ensure all processes and process-related artifacts are fully managed, reviewed and approved by DIR, SCP(s) or other approving entity as appropriate, and are stored in the SMM.

1.3.2.4 Facilitate and lead the automation or mechanization of processes between Successful Respondent and SCPs.

1.3.2.5 Design and deploy integrated technology and processes, as agreed, to automate DIR Shared Technology Services Enterprise Capabilities enabling efficient and effective execution, monitoring, and reporting of the supported IT services that shall be leveraged by DIR and DIR Customers.

1.3.2.6 Deploy controls to provide compliance positions of all enterprise processes across SCPs, DIR, and DIR Customers.

1.3.2.7 Ensure appropriate DIR Shared Technology Services policies and procedures are in place to ensure the security of the Infrastructure, Systems, Equipment, and DIR Data, including operating system security, layered product security, and enterprise software. This includes policies and procedures for SCPs to keep DIR Customer-used software and hardware versions current and supported. The Successful Respondent's duties include:

1.3.2.7.1 Establishing and enforcing security processes.

1.3.2.7.2 Ensuring all Authorized Users receive the security processes and requirements.

Exhibit 2.1 Statement of Work   Page 14

1.3.2.7.3 Reporting security related problems to DIR in accordance with the SMM and the governance risk and compliance process.

1.3.2.7.4 Implementing and monitoring access control authorizations in accordance with the SMM.

1.3.2.7.5 Reporting identified vulnerabilities in accordance with the SMM.

1.3.2.7.6 Maintaining a library of applicable security publications, such as ISO, NIST, FIPS and CJIS.

1.3.2.7.7 Facilitate SCPs to develop and maintain a process for the protection of all types of SCP backup media (e.g., tape, disk, removable).

1.3.2.8 Coordinate the execution of processes across SCPs, DIR, and DIR Customers in order that all individual components that make up IT Services are managed in an end-to-end manner.

1.3.2.9 Validate that the processes provide an audit trail that meets the legislative and policy requirements to which DIR must comply.

1.3.2.10 Communicate, train, and coordinate the policies and processes within Successful Respondent's own organization, SCPs, DIR, and Customers.

1.3.2.11 Provide on-going methods for training Successful Respondent personnel, SCPs, DIR, and DIR Customers on the DIR Shared Technology Services Enterprise Capabilities, including:

1.3.2.11.1 Prepare and maintain training content.

1.3.2.11.2 Publish content in the Successful Respondent-provided Learning Management System (LMS).

1.3.2.11.3 Administer the LMS, providing access to Successful Respondent personnel, DIR, DIR Customers, and SCPs.

1.3.2.11.4 Communicate course offerings to Successful Respondent personnel, DIR, DIR Customers, and SCPs.

1.3.2.12 Regularly provide guidelines, Frequently Asked Questions (FAQs), and provide access to appropriate tools to other SCPs, DIR, and DIR Customers to promote and reinforce the appropriate use of process escalation procedures.

1.3.2.13 Routinely evaluate the SCPs' and DIR Customers' effective compliance with the processes supporting the DIR Shared Technology Services Enterprise Capabilities.

1.3.3 Shared Services Reports

DIR expects the Successful Respondent to provide and maintain reports, metrics, and dashboards in support of the DIR Shared Technology Services Enterprise Capabilities noted in Table 1: MSI Shared Services Systems under the role of Platform.

This includes the ability for DIR to develop and generate its own ad-hoc reports as necessary. The MSI shall provide reports per the format and timing agreed with DIR as described in

Exhibit 2.1 Statement of Work
Page 15

Exhibit 3.4 Performance Analytics in support of all DIR Shared Technology Services Enterprise Capabilities processes and its **Attachment 3.4A Reports**.

1.3.3.1   The Successful Respondent shall provide a near real-time, web accessible reporting dashboard.

1.3.3.2   The Successful Respondent shall consult with DIR to establish the final content of the dashboard and shall document the specifications of the dashboard reports in the Transition Plan (see **Exhibit 3.3 Critical Deliverables**).

1.3.4   Shared Services Training

The Successful Respondent is responsible for providing the Shared Services learning management platform and leading in the creation, publishing, and tracking of web-based and webinar training content.

1.3.4.1   Training for DIR, SCPs, and Customers

The Successful Respondent shall, at a minimum:

1.3.4.1.1   Create, publish, schedule, provide, and maintain training courses to educate SCPs, DIR, and DIR Customers on the tools and processes within the DIR Shared Technology Services Enterprise Capabilities operations (e.g., Shared Services Overview, Portal Overview, Service Catalog, Incident Management, Configuration Management, etc.).

1.3.4.1.2   Create, publish, schedule, provide, and maintain training courses to educate SCPs, DIR, and DIR Customers on key topics required to support the DIR Shared Technology Services Enterprise Capabilities operations (e.g., Health Insurance Portability and Accountability Act (HIPAA) Security and Privacy, Federal Tax Information (FTI) Disclosure Awareness Training (Pub. 4711), Family Educational Rights and Privacy Act (FERPA), TAC 202).

1.3.4.1.3   Provide training to new Authorized Users and ongoing training to existing Authorized Users.

1.3.4.1.4   Provide electronic and online methods including webinar-type training as appropriate with, at a minimum, the ability to be accessed through Personal Computer (PC) or mobile devices.

1.3.4.1.5   Provide text, graphics, audio, animation, and/or video.

1.3.4.1.6   Provide interactive Question and Answer (Q&A) sessions, quizzes, and exams.

1.3.4.1.7   Provide the ability to track all aspects of a user, including: assigned, overdue, enrolled, started, completed, and exams passed/failed.

1.3.4.1.8   Continually investigate and analyze Authorized User training needs. Such analysis will be performed with the objectives of increasing customer satisfaction, improving quality of service, and increasing DIR Shared Technology Services growth.

1.3.4.1.9   Customize course content so that it is specific to the Authorized Users for the Services within the Shared Services environment.

Exhibit 2.1 Statement of Work   Page 16

    1.3.4.1.10 Provide multiple levels of training for specific MSI-applications (e.g., beginner and intermediate training in standard applications used by Authorized Users and provided as part of Services).

    1.3.4.1.11 Reporting on the effectiveness of such training and the metrics associated with each staff that was assigned, overdue, enrolled, started, completed, and passed/failed exams. Upon request, the Successful Respondent shall provide such documentation and training to DIR and SCPs as specified by DIR.

1.3.4.2   Training for MSI Personnel

The Successful Respondent shall maintain documentation and training material for its own personnel. At a minimum, the Successful Respondent's responsibilities include:

    1.3.4.2.1   Creating, maintaining, and delivering training that includes, at a minimum, the following information:

        1.3.4.2.1.1 The Services being provided;

        1.3.4.2.1.2 The value of these Services to DIR;

        1.3.4.2.1.3 The Contract structure and financial structure of Charges;

        1.3.4.2.1.4 Orientation and summaries on DIR, DIR Customers, SCPs, DIR Security Policies;

        1.3.4.2.1.5 Orientation to all applicable laws and regulations (e.g., TAC 202, HIPAA, etc.);

        1.3.4.2.1.6 The structure and location of the SMM; and

        1.3.4.2.1.7 All MSI systems and processes.

    1.3.4.2.2   Ensuring that all training material meets the minimum requirements for preparing Successful Respondent's personnel to support the delivery of Services.

    1.3.4.2.3   Providing proof that all Successful Respondent personnel interacting with DIR, DIR Customers, or SCPs have passed the required training.

    1.3.4.2.4   Reporting on the effectiveness of such training and the metrics associated with each staff that received training. Upon request, the Successful Respondent shall provide such documentation and training to DIR and SCPs as specified by DIR.

2   MARKETPLACE

2.1   Collaboration

DIR requires the Successful Respondent implement and maintain collaboration capabilities including a Portal, Document Repository, and Training System to be used as the centralized destination point of access to all documentation, shared information, system links, and broadcast communications pertaining to the delivery of the Services.

2.2	Portal

2.2.1   Portal System

The Successful Respondent shall propose a Portal design for DIR approval in the one-time Critical Deliverable "Public and Private Portal Design" defined in **Exhibit 3.3, Critical Deliverables**. The availability of Portal systems will be measured by the Critical SLA "MSI Shared Services Systems Availability," defined in **Exhibit 3.1 Service Level Matrix** and **Exhibit 3.2 Service Level Definitions.**

The Successful Respondent shall:

2.2.1.1   Design and implement a Portal that will be the centralized point of access to all processes, documentation, Portal broadcast communications, DIR Shared Technology Services tool links, and information pertaining to the delivery of Services.

2.2.1.2   Design and implement a public facing version of the Portal for potential DIR Customers (those not yet purchasing Shared Services), communicating Shared Services descriptions, solutions, technologies, problems solved, and value, including Successful Respondent contact information for visitors to seek additional information. The Portal design and implementation plan are subject to DIR approval.

2.2.1.3   Ensure that the Portal integration and information formats (e.g., web site, reports, etc.) are compliant with approved design standards and viewable by all stakeholders. Applications developed by the Successful Respondent and used by Texas state employees or members of the public must comply with Electronic and Information Resources (EIR) accessibility technical standards as defined in 1TAC 206. 50, 1TAC206.70, 1TAC 213, and Web Content Accessibility Guidelines (WCAG) 2.0 level AA. The Successful Respondent shall evaluate accessibility compliance when the Portal is established and each time thereafter when the Portal is enhanced. The Successful Respondent shall provide DIR evidence of accessibility compliance.

2.2.1.4   Provide for secure access to information by Authorized User role (e.g., DIR, Customers, SCPs, etc.) per DIR guidelines as specified in the SMM.

2.2.1.5   Provide secure access for DIR Customers to view and access DIR Customer-specific information which cannot be visible to other DIR Customers.

2.2.1.6   Ensure that the Portal content is accessible through both PC and mobile access (e.g., smart phone, tablet, etc.) providing access to Portal content, Service Catalog items, and service status (e.g., Incidents, Requests, Changes, etc.).

2.2.1.7   Provide that the Portal will allow users to login only once to access all permitted Portal functionality per profile and provide a secure single point of access validation to associated systems (i.e., single-sign-on).

2.2.1.8   Provide single-sign-on capabilities to enable user access to systems provided by the Successful Respondent and by appropriate systems provided by the SCPs.

Exhibit 2.1 Statement of Work   Page 18

2.2.1.9   Ensure that the Portal carries the approved DIR brand.

2.2.1.10 Provide capability for DIR Customers to receive notification when special DIR Customer-specific reports (e.g., Disaster Recovery Test, Demand Forecast, Security Exception) are available on the Portal.

2.2.1.11 Provide capability to create, publish, view, and download content as appropriate, by DIR Customer, Shared Service, Successful Respondent, and SCP.

2.2.1.12 Provide a repository to store and manage all DIR Shared Technology Services documentation, including the SMM, knowledge bases of Services, known errors and workarounds, training content, FAQs, and similar documentation for the Successful Respondent's organization as well as from other SCPs as specified by DIR.

2.2.1.13 Under DIR's direction, provide the ability for SCPs, DIR and DIR Customers to effectively share data. Limit access to data by role.

2.2.1.14 Test all user interfaces and output, and ensure that, at a minimum:

2.2.1.14.1 All Web based pages using HTML, XHTML, and/or Cascading Style Sheets (CSS) are validated using the appropriate W3C validation service (see http://www.w3c.org/)

2.2.1.14.2 Ensure that the Portal is compliant to Federal and State laws for Accessibility including Section 508 compliance (with §1194.22 Web-based Intranet and Internet Information and Applications) and Web Content Accessibility Guidelines (WCAG) 2.0 Level AA, and provide validation documentation of compliance.

2.2.1.15 Update the Portal to comply with future laws and rules as they are adopted, in accordance with the change management process.

2.2.1.16 Ensure that the Portal contains, at a minimum:

2.2.1.16.1 Access to the SMM and any other operational documentation describing the DIR Shared Technology Services Enterprise Capabilities, SCP, and DIR Customer-specific processes and operations.

2.2.1.16.2 Access to Shared Services communications describing various topics such as service offerings, new features, enterprise-wide system outages and other broadly distributed communications.

2.2.1.16.3 Access to all reports posted to the Portal and links to the Successful Respondent-provided enterprise reporting systems.

2.2.1.16.4 Organizational and contact information for Successful Respondent, DIR, and SCPs as approved by DIR.

2.2.1.16.5 Access to calendar containing important schedules and dates (e.g., governance meetings, change management meetings, billing invoice dates, etc.) at a level of detail as required by DIR.

Exhibit 2.1 Statement of Work   Page 19

2.2.1.16.6 Access to training materials and courses on all DIR Shared Technology Services Enterprise Capabilities that Successful Respondent, DIR, DIR Customers, and SCPs utilize.

2.2.1.16.7 Links to all systems provided by the Successful Respondent and appropriate systems provided by the SCPs.

2.2.1.16.8 Access to intuitive self-help and FAQ capability to allow users to answer their own questions and resolve their own issues.

2.2.1.16.9 Ability to search for and click to retrieve any content provided on the Portal according to the Authorized Users permissions.

2.2.1.16.10 Make other information, as mutually agreed upon during the Term, available through the Portal.

2.2.2 Portal Operations

The Successful Respondent shall provide and perform the roles to collect, copy edit, and publish Portal content in support of DIR and SCPs. The quality and effectiveness of Portal operations will be measured through Customer Scorecard feedback defined in **Exhibit 3.5 Customer Satisfaction** and Growth in Shared Services KPI defined in **Exhibit 3.4 Performance Analytics.** The effectiveness of Portal Operations will also be measured against the Service Management Manual process and procedures.

The Successful Respondent's responsibilities include, at a minimum:

2.2.2.1.1 Leading and facilitating the collection, copy editing, and publishing of content from DIR, Dir Customers, and SCPs and ensuring that it is accurate and clearly conveys the intended meaning.

2.2.2.1.2 Copy editing content to ensure the content is formatted per DIR-approved style guides and has correct grammar, spelling, and punctuation.

2.2.2.1.3 Obtaining content approval as required by DIR, DIR Customers, and SCPs.

2.2.2.1.4 Publishing and broadcasting accurate and timely Portal content.

2.2.3 Portal Management

The Successful Respondent shall ensure the integrity of Portal content and provide oversight to ensure the Portal is providing effective and efficient information across the DIR, Customer, and SCP user base. The quality of the Portal management will be measured against the one-time Critical Deliverable "Portal Content Management Plan" defined in **Exhibit 3.3, Critical Deliverables.**

The Successful Respondent shall, at a minimum:

2.2.3.1 Develop and maintain a Portal Content Management Plan specifying the Portal objectives and content update timing, editorial policies, style guides, and publishing requirements.

2.2.3.2 Lead and facilitate the development and maintenance of Portal content.

2.2.3.3 Lead and facilitate the approval of Portal content.

Exhibit 2.1 Statement of Work   Page 20

2.2.3.4   Lead and facilitate Portal content escalated issues.

2.2.3.5   Lead and facilitate the identification of initiatives to improve Portal effectiveness and usability.

2.2.3.6   Measure and report on content satisfaction, accuracy and timeliness.

2.3   Service Catalog Management

Service Catalog Management ensures the effective operation and management of the Service Catalog that includes DIR-approved services. The goal of the Service Catalog is to improve the end user experience when researching, ordering, and checking on the status of an order; therefore, the Service Catalog must be intuitive and accurate. The Successful Respondent shall provide the Service Catalog platform, operations, and management supporting the coordination and integrity of Service Catalog Content.

Service Catalog Management effectiveness will be identified in the Operational Metrics and related Service Catalog Management Critical SLA defined in **Exhibit 3.1, Service Level Matrix** and **Exhibit 3.2, Service Level Definitions.** The effectiveness of Service Catalog Management will also be measured against the Service Management Manual process and procedures. The availability of Service Catalog Management systems will be measured by the Critical SLA "MSI Shared Services Systems Availability," defined in **Exhibit 3.1 Service Level Matrix** and **Exhibit 3.2 Service Level Definitions**

The Successful Respondent shall:

2.3.1   Service Catalog System

2.3.1.1   Implement and maintain a Service Catalog for all DIR Shared Technology Services providing an intuitive, consumer-like storefront for users across one (1) to many service catalogs.

2.3.1.2   Ensure Authorized Users have access to only those Service Catalog items for which they are authorized.

2.3.1.3   Provide self-provisioning capability for Authorized Users to place orders.

2.3.1.4   Provide the capability to price selected services and orders prior to completing an order.

2.3.1.5   Provide self-help interface with service information (e.g., description, fulfillment times, pricing) to assist the user in searching and determining the appropriate service and features to order.

2.3.1.6   Ensure the Service Catalog is accessible through both PC and mobile access (e.g., smart phone, tablet) providing access to Service Catalog items and service fulfillment status.

2.3.1.7   For each Service Catalog item maintain, at a minimum:

    2.3.1.7.1   Item descriptions at a level of detail allowing users to make an informed purchase decision.

Exhibit 2.1 Statement of Work   Page 21

2.3.1.7.2 Commercial details, including pricing, terms, and chargeback description per Service Catalog item along with any prerequisite items.

2.3.1.7.3 Delivery timeframe including inventory on-hand as applicable.

2.3.1.7.4 Approval authority required to obtain the service, equipment, or software.

2.3.1.7.5 Technical specifications and configuration requirements including prerequisites or technical limitations for use or delivery of the service.

2.3.1.7.6 A description of how to obtain additional information about the service, equipment, or software.

2.3.1.8 Enable user input of attributes required to drive requests and integrate with the Request Management System to enable efficient order fulfillment across all SCPs and CSPs.

2.3.1.9 Ensure the Service Catalog System will interface with DIR and all SCPs' fulfillment systems.

2.3.1.10 Allow for standardized approval workflows with variables for which values are unique to a Customer.

2.3.1.11 Enable user input of attributes required to shop and order cloud services, including providing the user the ability to:

2.3.1.11.1 Modify any attribute of cloud services that can be modified by user.

2.3.1.11.2 Request the immediate decommissioning of cloud instances. The Successful Respondent shall cease billing upon approved user submission of the decommission request and the cloud provider's service decommission policies.

2.3.1.11.3 Add multiple Services into a Service Request.

2.3.1.11.4 Compare Services from multiple SCPs in a table format with pricing displayed for each offering.

2.3.1.11.5 Modify a Service Request's content (add/modify/remove) before submitting the Request.

2.3.1.11.6 Select a previous Service Request and use as a template to create a new request.

2.3.1.11.7 Print submitted Service Request.

2.3.1.11.8 Provide a "Review your Service Request" screen display prior to final submission with an action required to submit the service request. A message must indicate that user agrees to all applicable Charges upon submitting request.

2.3.1.11.9 Display a confirmation, pricing, and summary of what has been submitted once a user submits the service request.

2.3.1.11.10 Notify user when a service request is submitted and upon completion.

2.3.1.12 Provide a limited Internet-facing, Public Service Catalog in which orders may be placed for certain services, and allows for public facing access of select catalog items, in which:

Exhibit 2.1 Statement of Work   Page 22

2.3.1.12.1 Prospective DIR Customers may view available DIR Shared Technology Services including service descriptions, pricing, and terms as approved by DIR.

2.3.1.12.2 Provide FAQ information and other content to educate prospective DIR Customers on DIR Shared Technology Services.

2.3.1.12.3 Provide functionality to allow for users to order certain services, as defined by DIR, or initiate Contact Us emails to request additional information.

2.3.1.13 Provide an Authorized User a dashboard of user's service requests, relevant summary of active services along with pricing.

2.3.2 Service Catalog Operations

The Successful Respondent shall provide and perform the roles to design, implement, enhance, and manage Service Catalog items in support of DIR and SCPs. The Successful Respondent shall:

2.3.2.1 Create and actively maintain (at a minimum on a monthly basis) a list of the approved products and Services provided by all SCPs and the Successful Respondent for purchase or lease by Authorized Users within the Service Catalog.

2.3.2.2 Coordinate SCP requirements and manage all additions and updates to the Service Catalog with SCPs and DIR, subject to DIR approval.

2.3.2.3 Categorize Service Catalog contents by type of service, configuration type, equipment or software type, and user eligibility in order to enable multiple selection, searching, and presentation views (e.g., by DIR Shared Service, by product, by SCP, etc.).

2.3.2.4 Create and distribute regular communications with DIR and DIR Customers on updates to the Service Catalog, as approved by DIR.

2.3.2.5 Develop service descriptions for all services available on the Service Catalog and post these descriptions to the public and private portal for prospective and current Customers.

2.3.2.6 Publish and make available all Services in the Service Catalog to Authorized Users as directed by DIR.

2.3.2.7 Implement, manage, and maintain all Application Program Interfaces (APIs) required to keep the Service Catalog current and orchestrate Service provisioning across Service Providers.

2.3.2.8 Provide the capabilities for Authorized Users to compare public cloud offerings, review pricing, and place orders to request service in accordance with DIR procurement policies and standards.

2.3.2.9 Lead the SCPs and public cloud provider to design service catalog offerings. Provide expertise to configure and support the workflow to connect to and provision services

Exhibit 2.1 Statement of Work   Page 23

with public cloud providers.

2.3.2.10 Where appropriate, provide the capabilities for authorized Customers to select approved Software as a Service (SaaS) Products.

2.3.3 Service Catalog Management

The Successful Respondent shall perform roles to ensure the integrity of Service Catalog content and provide oversight to ensure the Service Catalog is providing effective and efficient information across the DIR, DIR Customer, and SCP(s) user base. The Successful Respondent shall:

2.3.3.1 Develop and maintain a Service Catalog Management Plan specifying the Service Catalog objectives, update timing, style guides, and publishing requirements.

2.3.3.2 Lead the development and maintenance of Service Catalog content, project managing required SCP tasks.

2.3.3.3 Lead the effort to obtain DIR approval of Service Catalog items and workflow.

2.3.3.4 Lead the resolution of Service Catalog related escalated issues.

2.3.3.5 Identify initiatives to improve Service Catalog effectiveness and usability.

2.3.3.6 Measure and report on Service Catalog satisfaction, accuracy and timeliness.

2.3.3.7 Create and maintain a list of the approved products and services provided by all SCPs for purchase or lease by Authorized Users

2.4   IT Service Desk and Constituent Help Desk

The Successful Respondent shall support two (2) service desks:

- **IT Service Desk** – Coupled with the Service Catalog, the Successful Respondent's IT Service Desk shall be the single point of contact for internal Services operational management handling contacts and coordinating the Event Management, Incident Management, Request Management and Access Management activities for DIR, Customers, and SCPs. The users contacting this service desk are referred to as **Authorized Users**.

- **Constituent Help Desk** – The single point of contact for citizens of the State regarding Incidents, requests and questions relating to State provided services (i.e., Texas.Gov). The citizens contacting this help desk are referred to as **Constituent Users**.

In the requirements for this Section, the term **Service Desk** refers to both desks (IT Service Desk and Constituent Help Desk) and the term **Service Desk User** refers to a Constituent User, Authorized User, DIR, the Successful Respondent, SCPs or anyone that can contact either of the Service Desks.

While each Service Desk supports a different set of customers, the underlying platform is common and requirements are consistent. The primary difference is the IT Service Desk is

Exhibit 2.1 Statement of Work   Page 24

highly coordinated with the Service Catalog to drive self-help while Constituent Help Desk customers initiate contact through telephone, email, and chat.

Service Desk and Help Desk service quality, timeliness and effectiveness will be measured through the Key SLAs defined in **Exhibit 3.1, Service Level Matrix** and **Exhibit 3.2, Service Level Definitions,** and through Customer Satisfaction and Scorecard measurements defined in **Exhibit 3.5, Customer Satisfaction.** The effectiveness of Service Desk and Help Desk Operations will also be measured against the Service Management Manual process and procedures. The availability of Service Desk and Help Desk systems will be measured by the Critical SLA "MSI Shared Services Systems Availability," defined in **Exhibit 3.1 Service Level Matrix** and **Exhibit 3.2 Service Level Definitions**

The Successful Respondent shall:

2.4.1   Service Desk Systems and Processes

2.4.1.1   Provide a Service Desk with processes that are ITIL-conformant, including the use of DIR and DIR Customer-provided Service Desk attendant scripts for supporting Incidents and service requests related to services, applications, systems, etc.

2.4.1.2   Effectively implement and use the capability for Authorized Users to submit Incidents and Service Requests via Service Catalog, telephone, chat, email, or other means approved by DIR.

2.4.1.3   Effectively implement and use the capability for Constituent Users to submit Incidents and Service Requests via telephone, chat, email, or other means approved by DIR.

2.4.1.4   Implement a knowledge base to assist with the resolution of Incidents and the processing of Service Requests, including:

    2.4.1.4.1   Make the knowledge base available on the Portal to Authorized Users for user self-help.

    2.4.1.4.2   Track the use of the knowledge base and report usage statistics to DIR on a monthly basis, or as requested by DIR (i.e., the number of Incidents resolved using the knowledge base).

2.4.1.5   Provide the capability to conduct end-user surveys of Service Desk Satisfaction as described in **Exhibit 3.5 Customer Satisfaction**.

2.4.1.6   Routinely educate Authorized Users on the use of the means to submit Incidents, Service Requests, and access the knowledge base with emphasis on the benefits of digital platform communications.

2.4.1.7   Effectively implement and use the capability for the Constituent Help Desk to identify and exclude or redact unsolicited Personally Identifiable Information (PII) and train service desk agents to recognize and appropriately handle unsolicited PII.

2.4.2   Service Desk Operations

Exhibit 2.1 Statement of Work   Page 25

2.4.2.1   Provide appropriate telecommunications capabilities to support Service Desk operations, including:

    2.4.2.1.1   Provide a single, toll-free (in-country) telephone number for external calls to the Service Desk from Authorized Users.

    2.4.2.1.2   Provide a single, toll-free (in-country) telephone number for external calls to the Service Desk from Constituent Users.

    2.4.2.1.3   Provide a single, toll-free (in-country) telephone number for external calls to the Service Desk from DPS Vehicle Inspection Connection (VIC) Users.

    2.4.2.1.4   Provide DIR with an alternative local number (in-country) for calls to the IT Service Desk and Constituent Help Desk agents.

2.4.2.2   Provide appropriately skilled personnel to execute Service Desk roles on a 24x7 basis.

2.4.2.3   Provide Successful Respondent Service Desk personnel to support the IT Service Desk, including:

    2.4.2.3.1   Provide English-language verbal and written support for the Service Desk, including voice, email, and chat communication.

    2.4.2.3.2   Provide clearly understandable communications, both spoken and written, to Authorized Users and SCPs.

2.4.2.4   Provide Successful Respondent Service Desk personnel to support the Constituent Help Desk, including:

    2.4.2.4.1   Provide English and Spanish-language verbal and written support for the Service Desk, including voice, email, and chat communication.

    2.4.2.4.2   Provide additional verbal language translation support through a tool or live translation service for the languages defined in the SMM: .

2.4.2.5   Provide clearly understandable communications, both spoken and written, to the Service Desk User and SCPs.

2.4.2.6   Provide Successful Respondent Service Desk personnel that are trained for the following:

    2.4.2.6.1   Possess the appropriate competencies and language skills to provide Service Desk services.

    2.4.2.6.2   Understand DIR's business, service levels, and its customers and respond appropriately.

    2.4.2.6.3   Understand DIR's, DIR Customers', and SCPs' technology and sourcing arrangements.

    2.4.2.6.4   Use recognized customer service and interpersonal skills, such as telephony skills, communication skills, active listening, and customer care training.

    2.4.2.6.5   Make appropriate decisions and initiate actions that reflect DIR and DIR Customer priorities.

Exhibit 2.1 Statement of Work   Page 26

2.4.2.6.6   Understand changes in products and services, as they become part of Successful Respondent's responsibilities.

2.4.2.6.7   Provide support to Authorized Users on both a reactive and a proactive basis, and for both in-bound and out-bound support.

2.4.2.7   Resolve Incidents and Service Requests from Service Desk Users relating to services in the approved Successful Respondent Shared Services System, including the following:

2.4.2.7.1   Receive and record all Incidents and Service Requests (including submissions received by telephone, electronically, or other means approved by DIR) in an Incident Record or Service Request Record, as appropriate, including classification and initial support.

2.4.2.7.2   For those that can be resolved at the Service Desk, resolve Incidents and Service Requests requiring Tier 1 support, and close after receiving confirmation to close from the affected Authorized or Constituent User, or, Successful Respondent.

2.4.2.7.3   Provide first-line investigation and diagnosis, to the maximum extent possible.

2.4.2.7.4   Assign Incidents and Service Requests that cannot be resolved to Tier 2 support within agreed timescales.

2.4.2.7.5   Assist by redirecting, as reasonable, Service Desk Users that have contacted the wrong Service Desk.

2.4.2.7.6   As defined in the SMM, communicate with Service Desk Users, keeping them informed of progress, notifying them of impending actions, obtaining appropriate agreement, and in all ways engaging and communicating with them about Successful Respondent activities.

2.4.2.7.7   Make appropriate updates to the Successful Respondent Shared Services Systems (e.g., Incident Management, Service Request Management, Asset Inventory and Management, Configuration Management, etc.) in compliance with SMM-approved processes.

2.4.2.7.8   Ensure solution is designed to handle Incident volumes and Incident response targets.

2.4.2.7.9   Provide an effective means of using industry recognized methods to solution, measure, and monitor Service Desk requirements and staffing allocations to support and provide Services.

2.4.2.7.10   Ensure all communications, whether spoken or written, shall be clearly understandable to the Constituent and Authorized Users.

2.4.2.8   Manage all Incidents and Service Requests from Service Desk Users relating to services, including the following:

2.4.2.8.1   Assigning categorization and prioritization codes.

2.4.2.8.2   As defined in the SMM, communicating with Service Desk Users, keeping them informed of progress, notifying them of impending actions, obtaining appropriate agreement, and in all ways engaging and communicating with them about the status of their activities.

Exhibit 2.1 Statement of Work   Page 27

2.4.2.8.3 Ensure all resolved Incidents, Service Requests, and other contacts are closed.

2.4.2.9 Coordinate the execution of all Service Desk processes across SCPs, DIR, and Service Desk Users in order that all individual components that make up IT Services are managed in an end-to-end manner.

2.4.2.10 Facilitate SCP support for Service Desk Users on both a reactive and a proactive basis.

2.4.3 Service Desk Management

The Successful Respondent shall perform roles to ensure the integrity of the Service Desk processes and operations and provide oversight to ensure the Service Desk is providing effective and efficient services to all Service Desk Users. The Successful Respondent shall:

2.4.3.1 Develop and maintain a Service Desk Management Plan specifying the Service Desk objectives performance, improvement initiatives, and risks.

2.4.3.2 Develop and maintain Service Desk processes, procedures, and workflow.

2.4.3.3 Develop and document in the Service Management Manual processes regarding interfaces, interaction, and responsibilities between Tier 1 Support personnel, Tier 2 Support personnel, and any other internal or external persons or entities that may either submit an Incident or receive an Incident.

2.4.3.4 Resolve Service Desk-related escalated issues.

2.4.3.5 Develop and periodically update Service Desk escalation procedures, and make available in the Portal such procedures to designated Authorized Users upon DIR's review and approval.

2.4.3.6 Identify and implement initiatives to improve Service Desk effectiveness and usability.

2.4.3.7 Analyze Incident trends, and recommend and implement actions, with DIR's approval, to reduce Incidents, including:

2.4.3.7.1 Increase the availability of self-help capability, including online FAQs and help documentation for common problems across Service Desks.

2.4.3.7.2 Collate Incident information from Service Desk Users regarding suggested improvements to MSI's service, including but not limited to self-help capabilities.

2.4.3.7.3 Routinely develop and manage an Action Plan to address these improvements. Action Plan is subject to DIR's approval.

2.4.3.7.4 Report on progress and improvements made.

2.4.3.8 Measure and report on Service Desk satisfaction, accuracy and timeliness on a monthly basis.

2.4.3.9 Conduct random surveys of Authorized Users immediately after they have used the

Exhibit 2.1 Statement of Work   Page 28

Service Desk in accordance with the SMM and Customer Satisfaction Survey requirements in **Exhibit 3.5 Customer Satisfaction**, and make available to DIR each month on the platform dashboard.

2.4.3.10 Conduct surveys of Constituent Users in accordance with the SMM and Customer Satisfaction Survey requirements in **Exhibit 3.5 Customer Satisfaction**, and make the survey data available to DIR each month on the platform dashboard. Notify SCPs in advance of the survey and provide survey results to the appropriate SCPs.

2.4.4   Service Desk User Instructions and Frequently Asked Questions (FAQs)

The Successful Respondent shall:

2.4.4.1   Identify potential Authorized Users' training requirements, and take action to address.

2.4.4.2   Provide and maintain instructions for Authorized Users and Constituent Users to access Services.

  2.4.4.2.1   The Successful Respondent shall make instructions available to Authorized Users via the Portal and agreed communication channels as requested by DIR.

  2.4.4.2.2   The Successful Respondent shall make instructions available to Constituent Users via other agreed online media as supported by the respective SCPs.

2.4.4.3   Provide and routinely update a list of FAQs regarding the Services on the Portal for Authorized Users and other online media.

2.4.4.4   Provide a list of FAQs regarding the Services for Constituent Users to the appropriate SCP for publishing on the Texas.gov site.

2.4.4.5   Publish answers to the FAQs using a media that is efficient, easy to use, and easily accessible for Authorized Users, as well as subject to approval by DIR.

2.4.4.6   Compile lists of FAQs where recommended solutions can be made available to Authorized Users to increase Authorized Users' ability to Resolve Incidents and handle Service Requests.

2.4.4.7   Publish FAQs lists for DIR, DIR Customers, and Constituents.

2.4.4.8   Provide FAQs in a format that can easily be published on DIR's, DIR Customers', and SCPs' internal systems.

2.5   Communications

The Successful Respondent shall coordinate and provide broad communications support across SCPs and Customers to ensure common messaging for DIR Shared Technology Services. The Successful Respondent shall, at a minimum:

Exhibit 2.1 Statement of Work   Page 29

1. Coordinate across all Service Providers to prepare unified internal communications to existing Customers and Service Providers (e.g., town hall presentations, newsletters, podcasts).

2. Track and provide awareness of industry award programs where DIR Shared Technology Services are eligible, and lead the development and preparation of external award applications.

Maintain on the Portal a repository of all communications distributed to Customers and Service Providers available for all Customers and Service Providers to reference.

Manage and publish content to the Portal (e.g., news and information, announcements), ensuring the messaging is consistent with other Customer communications.

2.6 Outreach and Growth

Customer outreach campaigns are required to drive the growth of all DIR Shared Technology Services across all DIR Customer segments (state agencies, local government, higher education). The Successful Respondent shall perform a lead role in analyzing new customer and new service opportunities, and coordinating outreach and implementation of DIR Shared Technology Services across current and potential DIR Customers. As new DIR Customer opportunities arise, the Successful Respondent shall track the opportunity through the outreach process and lead SCPs through the outreach, solution design, cost estimation and implementation processes.

The Successful Respondent shall provide outreach support for each DIR Shared Service and the state agencies participating in the Texas.gov offering. A Texas.gov SCP will provide the constituent-facing marketing and advertising services.

The Successful Respondent's performance in outreach and growth services will be measured against the Customer Outreach Plans required in **Exhibit 3.3, Critical Deliverables,** and against performance measures defined in **Exhibit 3.4, Performance Analytics**. Critical SLAs for New Service Offering Request Fulfillment and Onboarding Request Fulfillment – Customer/Service Component Provider, defined in **Exhibit 3.1, Service Level Matrix** and **Exhibit 3.2, Service Level Definitions**, will measure the effectiveness of the Successful Respondent's ability to incorporate new customers and new services. The outcome of the MSI outreach and growth services is the increase in customers and shared service offerings.

2.6.1 Outreach System

The Successful Respondent shall, at a minimum:

2.6.1.1 Lead and create an outreach campaign management process for DIR Shared Technology Services and implement and support the process within the Successful Respondent-provided Outreach System.

2.6.1.2 Lead and create a solutioning and costing process for DIR Shared Technology Services, and implement and support the process within the Successful Respondent's Systems.

2.6.1.3 Integrate the outreach processes and system with the Customer Relationship Management processes and systems to provide an end-to-end view of current and prospective DIR Customers.

Exhibit 2.1 Statement of Work   Page 30

2.6.2   Customer Outreach Development

2.6.2.1   The Successful Respondent shall lead in the creation and maintenance of annual outreach plans aimed at increasing the DIR Customer base for all DIR Shared Technology Services and the state agencies participating in the Texas.gov offering. At a minimum, the outreach plans shall contain:

    2.6.2.1.1   Definition, size, and segmentation of the potential customers for all DIR Shared Technology Services.

    2.6.2.1.2   Analysis on prospective DIR Customers for all DIR Shared Technology Services to be used as potential new DIR Customer leads.

    2.6.2.1.3   Evaluation of previous year's plan achievement and DIR Customer capture performance through documentation of actual outreach achievement as compared to the previous year's plan and prospective DIR Customer listing.

2.6.2.2   The Successful Respondent shall collaborate with SCPs in creating and maintaining a quarterly customer demand generation plan to drive awareness and interest in the DIR Shared Technology Services including the marketing channel plan and methods to engage prospective DIR Customers (e.g., website, social media, events, email blasts, etc.).

2.6.3   Campaign Management

The Successful Respondent shall lead and facilitate outreach campaigns by coordinating with DIR and SCPs to perform the following for each campaign:

2.6.3.1   Capture the outreach campaign objectives, services and target DIR Customers.

2.6.3.2   Define the campaign channels (e.g., Town Halls, Portal, or webinars for existing DIR Customers, social media, trade shows, website, or email for new external prospects) and organize the campaign.

2.6.3.3   Define measurements to track performance against the campaign objectives and implement the measurement.

2.6.3.4   Define the campaign plan, as approved by DIR, including timeline, roles, messaging, and collateral.

2.6.3.5   Program manage the outreach campaign plan execution coordinating across DIR, the Successful Respondent, and SCPs as required.

2.6.3.6   The Successful Respondent shall, when requested by DIR, conduct media purchases for use by SCPs and charge DIR as a pass-through.

2.6.4   Product Development

2.6.4.1   The Successful Respondent shall lead and facilitate, across DIR and the SCPs, the creation of product description collateral for use in driving demand and educating new and existing DIR Customers of the DIR Shared Technology Services and the state

Exhibit 2.1 Statement of Work   Page 31

agencies participating in the Texas.gov offering. At a minimum, the collateral shall:

2.6.4.1.1 Address topics such as: problem being solved, service and solution descriptions and benefits/value propositions

2.6.4.1.2 Be in multiple forms for convenient use in outreach activities, including at a minimum: presentations, case studies, white papers, data sheets, etc.

2.6.4.2 **NOTE**: The Successful Respondent is not responsible for any outreach, marketing, or sales to Texas constituents using Texas.gov. A Texas.gov SCP will lead and facilitate the product marketing collateral for constituent-facing collateral.

2.6.5 Solutioning

2.6.5.1 The Successful Respondent shall provide the capabilities through an externally-facing public service catalog to respond to demand generated from interested potential DIR Customer requests.

2.6.5.2 The Successful Respondent shall provide the capabilities for Successful Respondent representative to manage the SCP and prospective customer in the leads generated through outreach activities.

2.6.5.3 Program manage the Service, cost estimation and implementation activities across DIR, SCPs, and the DIR Customer.

2.6.6 Outreach Operations

2.6.6.1 The Successful Respondent shall log and track all DIR Customers from prospect implementation into delivery.

2.6.6.2 The Successful Respondent shall, at a minimum, track: Customer information, date, and purpose of captured contacts, actual and planned follow-ups, services interested in, cost estimates, requested due dates, status.

3 SERVICE MANAGEMENT

3.1 Incident Management

The Successful Respondent's Incident Management discipline shall encompass Incident Management processes deployed across the Successful Respondent and all SCPs, designed to: restore service as quickly as possible, enable and leverage automation capabilities across the Successful Respondent's and SCPs' Systems to fully automate Incident resolution, minimize disruption to DIR Customers' businesses, aim for best levels of availability and service quality, provide transparent and auditable delivery of service, and promote the highest level for user satisfaction.

Incident Management service effectiveness will be measured by Critical SLAs (Resolution Time, Time to Initiate a Major Incident Response Team) and Key SLAs (Incident Communication) defined in **Exhibit 3.1, Service Level Matrix** and **Exhibit 3.2, Service Level Definitions.** The effectiveness of the Successful Respondent's management of SCP incidents will be measured by

Exhibit 2.1 Statement of Work   Page 32

the Performance Analytics for Service Quality defined in **Exhibit 3.4, Performance Analytics.** Incident Management System. The availability of Incident Management systems will be measured by the Critical SLA "MSI Shared Services Systems Availability," defined in **Exhibit 3.1 Service Level Matrix** and **Exhibit 3.2 Service Level Definitions.**

3.1.1   Incident Management System

The Successful Respondent shall:

3.1.1.1   Deploy and utilize an Incident Management System that provides a level of sophistication allowing for a set of Incident Resolution diagnostics.

3.1.1.2   Track Services to enable the automation of monitoring, detection, prioritization, establishment of resolution times, and the Resolution of Incidents associated with the Services. The Successful Respondent shall, at a minimum:

3.1.1.3   Implement an automated Incident Management System, including the integration of applicable software, equipment, email, telephony, and Web technologies.

3.1.1.4   Maintain a central knowledge database used to capture, store, and retrieve information and solutions to resolve Incidents for use by Successful Respondent, SCPs, and Authorized Users.

3.1.2   Incident Management Processes

The Successful Respondent shall:

3.1.2.1   Develop and document in the Service Management Manual processes and procedures regarding interfaces, interaction, and responsibilities between Tier 1 support personnel, Tier 2 support personnel, Tier 3 support personnel, and any other internal or external persons or entities that may either raise an Incident, receive an Incident, or support the Resolution of Incidents.

3.1.2.2   Provide a mechanism for handling of Incidents according to the agreed to prioritization model used by DIR, DIR Customers, and SCP(s), based on the assigned Severity Level, in compliance with the Incident Management and Problem Management Processes described in the SMM.

3.1.2.3   Provide a mechanism for expedited handling and increased communication of Incidents that are of high business priority to DIR, DIR Customers, and SCP(s), based on the assigned Severity Level, in compliance with the Escalation Processes described in the SMM.

3.1.2.4   Develop an incident resolution escalation process for Successful Respondent and SCPs when progress is not being made in resolving high severity incidents.

3.1.3   Incident Management Operations

For Incidents the Successful Respondent can resolve, the Successful Respondent shall, at a minimum:

Exhibit 2.1 Statement of Work   Page 33

3.1.3.1   Perform all Incident resolution responsibilities in accordance with the Service Management Manual, knowledge database documents, and configuration database(s), including the following:

    3.1.3.1.1   Resolve Incidents in accordance with the Service Management Manual, knowledge database documents, and configuration database(s).

    3.1.3.1.2   Identify and classify Incident Severity and handle according to agreed-upon Incident response procedures and assume end-to-end responsibility to resolve.

    3.1.3.1.3   Leverage a knowledge base as described in SOW Section **3.2 Problem Management** to assist with the Resolution of Incidents and the processing of Service Requests.

    3.1.3.1.4   Participate in Incident review sessions.

    3.1.3.1.5   Track and report the progress of Resolution efforts and the status of all Incidents.

    3.1.3.1.6   Update the progress of an Incident's resolution within the Successful Respondent's tracking systems through to final closure.

    3.1.3.1.7   Update all associated records (e.g., contacts, other Incidents, asset inventory, configuration management records) are updated to reflect completed/resolved Incidents.

    3.1.3.1.8   Close Incident, including Service Requests, after receiving confirmation from the affected Authorized User, or Successful Respondent support personnel for Incidents reported via an event detection tool, that the Incident has been Resolved.

    3.1.3.1.9   Follow approved SMM guidelines for closure rules and procedures.

    3.1.3.1.10 Document solutions to resolved Incidents in Successful Respondent managed central knowledge base. Accurately update all information pertinent to Incident ticket including general verbiage, codes, etc.

    3.1.3.1.11 Determine wherever possible whether an Incident should initiate a Problem investigation (e.g., whether preventive action may be necessary to avoid Incident recurrence) and, in conjunction with the appropriate support tier, raise a Problem record to initiate action.

3.1.3.2   For Incidents, the Successful Respondent is unable to resolve, perform the following:

    3.1.3.2.1   Escalate Incidents to Tier 2 support according to the SMM.

    3.1.3.2.2   Perform the activities as specified in section 3.1.4 Management of Incidents.

3.1.4   Management of Incidents

For all Incidents, including those the Successful Respondent can resolve and those assigned to SCPs, DIR or DIR Customers, the Successful Respondent shall, at a minimum:

3.1.4.1   Provide a process to coordinate Incident Management activities across all functions and organizations, including the Successful Respondent, SCPs, DIR, and DIR Customers that provide services to DIR Customers.

Exhibit 2.1 Statement of Work   Page 34

3.1.4.2   Provide effective and agreed mechanisms for properly establishing the priority of Incidents based on established prioritization criteria (e.g., scripts, diagnostic tools, etc.).

3.1.4.3   Develop a process enabling all associated records (e.g., contacts, other Incidents, asset inventory, configuration management records) to be updated to reflect completed/resolved Incidents.

3.1.4.4   Where Incidents result in a Change in the IT environment, provide a process such that Changes can be initiated through the Change Management process as appropriate.

3.1.4.5   Where appropriate, the Incident scan should be automated, perform a data-driven analytical approach to scan Incidents prior to closure to ensure proper categorization, documentation, resolution, Authorized User interaction and closure actions are complete.

3.1.4.6   For Incidents not meeting closure criteria per criteria of above item, scan and initiate corrective actions to address the findings.

3.1.4.7   Ensure all appropriate parties are notified of the SLA allotted Resolution time for each Incident. Provide automated triggers to escalate an incident nearing the allotted Resolution time.

3.1.4.8   Coordinate Incident tracking efforts, and provide and maintain regular communications, per the SMM, between all parties and Authorized Users until Incident Resolution. Keep DIR Customer informed of anticipated Resolution times for active Incidents as defined in the SMM.

3.1.4.9   Keep DIR and Customer informed of changes in Incident status throughout the Incident lifecycle in accordance with the SMM.

3.1.4.10 Provide regular progress notifications to DIR and Customers on current Incidents for all Severity Levels. High severity incidents will require more frequent communication. The frequency of such notification is determined by the severity of the Incident as determined using the definitions given in **Exhibit 3.0 Performance Model**. The frequency of notifications shall be documented in the SMM and approved by DIR.

3.1.4.11 Provide prompt notification to DIR and DIR Customers of system outages on critical systems identified in the Incident Management System and otherwise provide affected Authorized Users with regular progress updates within designated timeframes, as prescribed in the Incident Management notification section of the SMM, that clearly indicate the following:

   3.1.4.11.1 Nature and scope of the Incident;
   3.1.4.11.2 Estimated time to completion; and
   3.1.4.11.3 Potential short-term alternatives.

3.1.4.12 Maintain communications and provide status reports to DIR and Customer, Service Desk and appropriate SCP(s) from the time an Incident is identified through Resolution,

Exhibit 2.1 Statement of Work   Page 35

and, as necessary, through any follow-up communication and work required post-resolution as defined in the SMM.

3.1.4.13 Develop, utilize, manage, and continually improve an inventory of defined and documented Incident models that incorporate at a minimum the following elements:

> 3.1.4.13.1 Sequences of tasks, actions or steps to execute the Incident model and resolve the Incident.
>
> 3.1.4.13.2 Identification of required dependencies, data sources, etc. that must be considered in executing the Incident model.
>
> 3.1.4.13.3 Definition of responsibilities and roles to execute the Incident model.
>
> 3.1.4.13.4 Timescales, milestones and thresholds for executing the Incident model.
>
> 3.1.4.13.5 Anticipated escalation points and escalation procedures associated with the Incident model.

3.1.5   Major Incident Management

Major Incidents are the highest severity for an Incident where the impact or potential impact to a critical business service necessitates a response above and beyond what is provided by the normal Incident Management Process. The expected outcome is a quicker resolution resulting in minimal disruption and maximum availability of services.

The timeliness to initiate Major Incident Management will be measured in the Critical SLA defined in **Exhibit 3.1, Service Level Matrix** and **Exhibit 3.2, Service Level Definitions.** The effectiveness of the Successful Respondent's management of Major SCP incidents will be measured by the Performance Analytics for Service Quality defined in **Exhibit 3.4, Performance Analytics.** The availability of Major Incident Management systems will be measured by the Critical SLA "MSI Shared Services Systems Availability," defined in **Exhibit 3.1 Service Level Matrix** and **Exhibit 3.2 Service Level Definitions**

The Successful Respondent shall, at a minimum:

3.1.5.1   For incidents identified by a DIR Customer through the Successful Respondent's Service Desk, assign the Incident to the appropriate resolver team and warm-transfer the Incident to a specific resolver. For incidents entered through the ITSM system, automate immediate notification to appropriate resolver teams.

3.1.5.2   Provide end-to-end responsibility and ownership for each Major Incident to an Incident Manager, thus minimizing redundant contacts with the Authorized User.

3.1.5.3   Notify the appropriate parties, in accordance with established SLAs and DIR-approved SMM procedures, including DIR, DIR Customers, the Successful Respondent, and SCPs of the Major Incident. Provide communication (email, ticket, etc.) that sufficiently explains the situation, options, research accomplished to date, etc., to stakeholders not directly participating in the incident resolution.

3.1.5.4   Monitor and lead Major Incident resolution by gathering all relevant information available pertaining to the Incident, monitoring the outage, inspecting for progress in the diagnosis, directing resolution teams, and documenting resolution attempts of the

Exhibit 2.1 Statement of Work   Page 36

resolver teams until the Major Incident is resolved. Evaluate the effectiveness of resolution efforts in progress and provide direction to minimize downtime and coordinate resolution teams.

3.1.5.5   During the Major Incident lifecycle, facilitating the identification of the steps to pursue, and identify communication needs and potential escalations. Monitor and direct the SCPs through the resolution process.

3.1.5.6   Establish escalation guidelines to be invoked when resolution has not been achieved at pre-defined checkpoints to ensure efficient and effective resolution.

3.1.5.7   In order to accelerate resolution, establish guidelines for when to require SCPs to seek Third Party Vendor support.

3.1.5.8   Formulate and manage a Major Incident restoration team consisting of any technical and managerial resources needed to work toward swift resolution. The team may include SCP(s), DIR Customer liaisons, the Successful Respondent or DIR representatives that may be necessary to work toward a quick resolution.

3.1.5.9   Provide, establish, and provision any supporting communication facilities (i.e., conference bridges, online work spaces, etc.) that may be required to support the effective facilitation of Incident diagnosis and resolution.

3.1.5.10 Manage and direct the Incident from identification to resolution, including, but not limited to, the following:

   3.1.5.10.1 Review the Resolution target for each Incident with the appropriate party and update the status accordingly.
   3.1.5.10.2 Coordinate Incident tracking efforts, and provide and maintain regular communications between all parties and Authorized Users until Incident Resolution.
   3.1.5.10.3 Keep DIR and DIR Customer informed of changes in Incident status throughout the Incident lifecycle, in accordance with Service Levels.
   3.1.5.10.4 Keep DIR Customer informed of anticipated Resolution times for active Incidents.
   3.1.5.10.5 As appropriate and per the DIR-approved SMM, facilitate the initiation of the crisis management plan.
   3.1.5.10.6 Maintain and document the Incident resolution by coordinating with the restoration team and ensuring the Incident documentation is accurate and up to date.
   3.1.5.10.7 Upon resolution, provide final update communications, according to procedures established in the DIR-approved SMM and in compliance with associated SLAs defined in **Exhibit 3.1, Service Level Matrix** and **Exhibit 3.2, Service Level Definitions**, informing all interested parties that the situation is resolved.

3.1.6   Incident Escalation

Exhibit 2.1 Statement of Work   Page 37

The Successful Respondent shall, at a minimum:

3.1.6.1 Provide an automated process for escalating to Successful Respondent's management for Incidents not Resolved in the time frames appropriate to the severity of the Incident and the priority of the user.

3.1.6.2 Escalate Incidents according to processes and procedures in the DIR-approved SMM.

3.1.6.3 Automatically prioritize high-impact Incidents, as defined by DIR, and treat with the highest priority as defined in the SMM.

3.1.6.4 Provide for emergency escalations to SCP or Third Party resources at the discretion of DIR.

3.1.6.5 Implement and operate escalation processes, as defined in the DIR-approved SMM, that reflect and describe, at a minimum, the following items:

  3.1.6.5.1 Severity Level of the Incident.
  3.1.6.5.2 Impact on affected Users (e.g., location of the Incident, names and/or number of users).
  3.1.6.5.3 Priority of the User (e.g., Executive Director, Legislative request, etc.).
  3.1.6.5.4 Elapsed time before an Incident is escalated for Resolution as if it were the next higher Severity Level.
  3.1.6.5.5 The levels of involvement (and notification), for escalation of Incidents, of Successful Respondent management and DIR and DIR Customer management at each Severity Level.
  3.1.6.5.6 Investigative and diagnostic activities to identify temporary workarounds for each Incident.
  3.1.6.5.7 Incident Resolution activities to restore normal service in compliance with the Service Levels.
  3.1.6.5.8 Ability to Resolve Incidents by matching Incidents to known errors that are stored in a Known Error Database.
  3.1.6.5.9 Ability to Resolve Incidents by implementing workarounds that are stored in a Known Error Database.
  3.1.6.5.10 Process used to escalate Incidents to appropriate support teams when necessary.
  3.1.6.5.11 Process used to escalate Incidents to Successful Respondent's management team and/or DIR's and DIR Customers' management team.

3.1.6.6 Track information regarding escalations to include frequency of usage by DIR Customers.

3.2 Problem Management

The Problem Management capability performs Root Cause Analysis (RCA) and initiates Corrective Actions to minimize the adverse effect Incidents have on the business by reducing

Exhibit 2.1 Statement of Work   Page 38

repeat Incidents and eradicating errors in the IT infrastructure, Applications, systems, and supporting components. Proactive Problem Management analyzes historical Incidents, problems, and trends to identify and address issues before they cause an Incident.

The effectiveness of Problem Management will be measured by the Critical SLAs (Root Cause Analysis Delivery and Corrective Actions), and the Key SLA Chronic Enterprise Incidents defined in **Exhibit 3.1, Service Level Matrix** and **Exhibit 3.2, Service Level Definitions.** The availability of Problem Management systems will be measured by the Critical SLA "MSI Shared Services Systems Availability," defined in **Exhibit 3.1 Service Level Matrix** and **Exhibit 3.2 Service Level Definitions**

3.2.1   Problem Management System

The Successful Respondent shall deploy and utilize a Problem Management System that provides the ability to track, monitor, prioritize problem investigations, RCA results, and implement Corrective Actions associated with the Services.

The Successful Respondent shall, at a minimum:

3.2.1.1   Design and build the Problem Management System to include the capabilities to support and execute the Problem Management process as defined in the DIR-approved SMM, including but not limited to:

   3.2.1.1.1   The ability to electronically link or associate Problems with related Incidents, Changes, Releases, and Configuration Items or components.

   3.2.1.1.2   Provide a Known Error Database or Knowledge Database that will be used for storing knowledge, records and information regarding previous Problems, Known Errors, workarounds and Incidents (including both diagnostic and Resolution information), and which will be available for use by all relevant stakeholders, including DIR, DIR Customers, and other SCPs.

3.2.1.2   Provide capabilities for the tracking and reporting of RCA and Corrective Action activities.

3.2.1.3   Regularly update the Problem Management System (including the Known Error Database/Knowledge Database) with the Successful Respondent and other SCP solutions and best practices as they are developed, including updates based on "lessons learned" and experience with similar technologies and problems for other customers.

3.2.2   Problem Management Operations

The Successful Respondent shall, at a minimum:

3.2.2.1   Provide means for Problem records to be created from all relevant sources, specifically including the following:

   3.2.2.1.1   The Service Desk;

   3.2.2.1.2   Incident Management;

   3.2.2.1.3   Enterprise Event Management;

   3.2.2.1.4   SCPs;

Exhibit 2.1 Statement of Work   Page 39

3.2.2.1.5 DIR and DIR Customers.

3.2.2.1.6 Proactive problem management.

3.2.2.1.7 Capacity Management and Availability Management processes.

3.2.2.2 Perform proactive data analysis on Incident, Problem, Corrective Action, Availability, and Capacity data processes to proactively perform Problem Management with the objectives of automating the Problem Management process and predicting Problems before they occur.

3.2.2.3 Coordinate Problem Management activities, as defined in the DIR-approved SMM, across all functions and organizations, including SCP(s), DIR and DIR Customers. The Successful Respondent shall perform the following coordinating activities, at a minimum:

3.2.2.3.1 Reviewing the Incident requests requiring problem investigations including ensuring Customer-requested problem investigations are defined to address the issue as stated by the Customer.

3.2.2.3.2 Ensuring the problem investigations are assigned to the right resolver team.

3.2.2.3.3 Ensure the priority of the problem investigation and associated Corrective Actions are properly set based on established prioritization criteria.

3.2.2.3.4 Ensuring that the problem investigations progress through the problem management process in a timely and prioritized fashion.

3.2.2.3.5 Lead problem investigations requiring cross-SCP RCA investigation and manage Corrective Action resolution.

3.2.2.3.6 Review completeness of problem investigations and ensure effective execution of RCA.

3.2.2.3.7 Conduct regularly scheduled Problem Management meetings to prioritize the Resolution of Problems across other SCPs.

3.2.2.3.8 Document and publish Problem Management meetings status reports to all relevant stakeholders, including DIR, DIR Customers, and SCP(s).

3.2.2.4 Verify and track that the identified Corrective Actions are being implemented.

3.2.2.5 Escalate to appropriate management within DIR, DIR Customers, the Successful Respondent, and SCP(s) if corrective actions are not being closed.

3.2.2.6 Update Known Error Database/Knowledge Database with all relevant information, including documented workarounds for Problems/Known Errors as they identified and addressed.

3.2.2.7 Provide support to SCP(s) to document workarounds for Incidents that can be used to support the handling of future Problems and Incidents, and will:

3.2.2.7.1 Be stored in the Known Error Database/Knowledge Database.

3.2.2.7.2 Be categorized in a manner like the categorization of Incidents and Problems in order to facilitate effective identification and use.

Exhibit 2.1 Statement of Work   Page 40

3.2.2.7.3 Provide a detailed description of the steps to be executed to implement the workaround.

3.2.2.7.4 Provide a detailed description of any required inputs, capabilities, resources, etc., that are required for proper execution of the workaround.

3.2.2.7.5 Describe the appropriate context under which the workaround is to be used and/or conditions under which it is not to be used.

3.2.2.7.6 Provide a reference to previous Incidents, Problems, and Known Errors to which the workaround is related.

3.2.2.7.7 Provide a reference to the service, system or configuration item/component to which the workaround is related.

3.2.2.8 Maintain accurate communications within designated SLA timeframes and provide status reports through the Service Desk, DIR, DIR Customers, and SCPs as necessary from the time a Problem is identified through Resolution.

3.2.2.9 Track and report any backlog of unresolved Problems on at least a monthly basis to the Problem Manager, or more frequently as requested by DIR.

3.2.3 Major Problem

The Successful Respondent shall, at a minimum:

3.2.3.1 Conduct Major Problem Reviews associated with Major Incidents, as described in the DIR-approved SMM, that arise or may arise out of the Services.

3.2.3.2 Coordinate all communications and notices for Major Problem Reviews to all relevant stakeholders, including SCPs, DIR, DIR Customers, and in compliance with the processes in the SMM.

3.2.3.3 Effectively execute Major Problem Reviews, in compliance with the processes defined in the SMM, which will include:

3.2.3.3.1 Assignment of a Problem Manager, including Major Incident Managers as appropriate, to facilitate the Major Problem Review.

3.2.3.3.2 An analysis of lessons learned from the Major Incident (e.g., things done well, things needing improvement, etc.).

3.2.3.3.3 A description of the associated Incident, including description of the failure, business impact, duration, affected systems, affected services, affected customers, work executed to Resolve the Incident, etc.

3.2.3.3.4 A detailed RCA of the Incident.

3.2.3.3.5 Identification of any Corrective Actions, Known Errors, and workarounds associated with or created.

3.2.3.3.6 Communication of findings and outcomes to all relevant stakeholders.

3.2.3.3.7 The identification, documentation, and submission of identified improvements.

3.2.3.3.8 Preventive action items tracked to completion, including regular communication with relevant stakeholders during the process.

Exhibit 2.1 Statement of Work   Page 41

3.2.3.3.9 Notice to all relevant stakeholders when preventative action items have been completed or missed.

3.3   Information Security Management

Confidential Security Information

3.4   Access Management

Access Management is focused on the platform, process and operations to enable Authorized Users to request access to and use an IT service.

3.4.1 DIR Shared Technology Services Access Management

The Successful Respondent shall, at a minimum:

3.4.1.1 Establish processes that properly route Access Requests across DIR Customers, the Successful Respondent, SCPs, and organizations.

3.4.1.2 Provide each SCP, DIR Customer, the Successful Respondent, and DIR, collectively referred to as Access Owners, the ability to specify instructions and exercise their authority for reviewing and approving access to their respective DIR Shared Technology Services systems and applications.

3.4.1.3 Implement, maintain, and follow the Access Owner's instructions for review and approving Access Requests.

3.4.1.4 Ensure all requests are executed within the security policies, procedures, and guidelines of DIR.

3.4.1.5 Provide near real-time notification to each Access Owner for all Access Requests, approved or denied, made to their respective DIR Shared Technology Services systems and applications.

3.4.1.6 Enable multiple mediums for accepting Access Requests, including the Service Desk, and Service Catalog.

3.4.1.7 Enable the use of online self-service to allow Authorized Users to enter Access Requests through a "menu"-type selection, so that they can select and input details of Access Requests from a pre-defined list.

3.4.1.8 Integrate with and leverage the Service Catalog Management, Request Management and IT Service Desk process and capabilities to execute the Access Management operations.

3.4.1.9 Integrate the Successful Respondent's Logical Security Administration process with DIR's, DIR Customers', and SCPs' Logical Security Administration processes, where the processes interact.

3.4.1.10 Establish and maintain mechanisms to safeguard against the unauthorized access,

Exhibit 2.1 Statement of Work   Page 42

destruction, loss, or alteration of DIR's and DIR Customers' data. The Successful Respondent shall implement safeguards that are no less rigorous than the practices performed by DIR and DIR Customers as of the Commencement Date.

3.4.1.11 Having obtained DIR approval, install, update, and maintain Software that will provide security monitoring, alarming, and access-tracking functionality for Successful Respondent-operated systems and Software.

3.4.1.12 Provide for security access controls for Successful Respondent-maintained and operated data, Software, and networks in compliance with DIR Security Policies, standards, and procedures as documented in the DIR-approved SMM; and maintain such security and access control devices in proper working order.

3.4.1.13 Develop, implement, and maintain a set of automated and manual processes designed to enforce DIR and Customer's data access and security policies and procedures.

3.4.1.14 In coordination with DIR IT Security, establish procedures, forms, and approval levels for assigning, resetting, and disabling IDs and passwords used for data or system access by Authorized Users.

3.4.1.15 Provide reports on violation and access attempts, and retain documentation of the investigation.

3.4.2   Successful Respondent-operated Systems Access Management

The Successful Respondent shall, at a minimum:

3.4.2.1   Administer access to Successful Respondent-operated systems, networks, and Software, to include the following:

  3.4.2.1.1   DIR, SCPs, and DIR Customers will notify Successful Respondent regarding the entities and personnel to be granted access to Successful Respondent-operated systems and the level of security access granted to each.

  3.4.2.1.2   Follow DIR's, SCP's, and DIR Customers' instructions and the procedures regarding such access as designated by DIR, SCP, or DIR Customers.

  3.4.2.1.3   Execute all approved administration for user IDs and passwords.

  3.4.2.1.4   Provide administration related to user IDs and passwords for Successful Respondent-operated systems.

  3.4.2.1.5   Regularly review account activity and disable inactive accounts.

  3.4.2.1.6   Communicate with Authorized Users regarding requests for system or data access, and process those requests with DIR, SCP, and DIR Customer IT Security, which authorizes access.

3.4.2.2   Manage access to Successful Respondent-operated systems, networks, Software, and Shared Services authorized systems, to include the following:

Exhibit 2.1 Statement of Work   Page 43

3.4.2.2.1 Upon request provide DIR IT Security full administrative rights related to systems regarding the Services, including full access to audit trails and logs.

3.4.2.2.2 DIR and DIR Customers will retain authority for approval of all data and system access requirements.

3.4.2.2.3 Ensure that the comprehensive database of security clearances and access rights is maintained and tracking all the logical access rights of Successful Respondent personnel to systems associated with providing the Services.

3.4.2.2.4 Review all documented information security procedures with DIR pertaining to Successful Respondent-operated systems.

3.4.2.2.5 Comply with DIR policies on privacy protection and protective security for data, including security, data and records management, and electronic records and data archiving.

3.4.2.2.6 Conform to the requirements in accordance with government guidelines and DIR and DIR Customer security policies.

3.4.2.2.7 Monitor users of the systems and Services for authorized access, and monitor, review, and respond in an appropriate manner to access violations within designated timeframes.

3.4.2.2.8 Provide near real-time information to DIR, SCPs, and DIR Customers to identify those accounts that should be removed on systems for Successful Respondent-operated systems.

3.4.2.2.9 Capture data regarding routine access and exceptions for audit trail purposes, ensure that time stamps are synchronized with a common time source for event correlation and make such data available to DIR or DIR Customers upon request.

3.4.2.2.10 Run periodic reports to identify accounts that should be removed/disabled or atypical usage of a particular Authorized User or group, and provide reports to DIR IT Security.

3.4.2.2.11 Coordinate system password changes and, subject to DIR or DIR Customers' approval, change, and test all local passwords as required.

3.4.2.2.12 Assist the SCPs in the development, testing, and utilization of an action plan and escalation procedures for any potential or real security breaches and report any potential or real security breaches to DIR, SCPs, or DIR Customers per the plan.

3.4.2.2.13 Document and identify security risks associated with the Services annually and provide mitigation strategies in the annual Security Plan.

3.4.2.2.14 Notify DIR and DIR Customers in the event of a security violation or unauthorized attempt to access or alter DIR or DIR Customer data, where the notification and escalation is made according to security policy guidelines and procedures.

3.4.2.2.15 Conduct semi-annual reviews, as appropriate, to validate and report to DIR and DIR Customers that individual employee access to programs and systems is appropriate for Successful Respondent-operated systems.

3.4.2.2.16 Intentionally left blank.

Exhibit 2.1 Statement of Work   Page 44

3.4.2.2.17 Perform security audits, provide Incident investigation support, and initiate corrective actions to minimize and prevent security breaches.

3.4.2.2.18 Perform backup and recovery procedures in response to security violations that result in lost/damaged information.

3.4.2.2.19 Respond to all security validation and audit requests from DIR and/or regulatory authorities.

3.4.2.2.20 Assist DIR, DIR Customers and/or representatives of DIR in executing security tests, identify remediation needs, and project manage the remediation activities. (e.g., validation efforts, audits, Third Party security tests, vulnerability scans, Penetration Tests, etc.).

3.4.2.2.21 With DIR's approval, change security in responses to evolving requirements and changing technology and related processes.

3.4.2.2.22 Establish and maintain safeguards against the unauthorized access, destruction, loss, or alteration of DIR or DIR Customer data in the possession of Successful Respondent, where the safeguards are at least as stringent as DIR policies.

3.5 Request Management and Fulfillment

The Successful Respondent shall be responsible for enabling and managing all requests for Services from DIR, DIR Customers, and SCPs, from the initial request through fulfillment of such requests via Services from multiple sources, such as other SCPs, DIR, or DIR Customers. Request management includes all types of Service Requests, including Requests for Solution (RFS), Report requests, etc.

The effectiveness of the Request Management and Fulfillment processes will be measured by Critical SLAs (New Service Request Fulfillment, Onboarding Request Fulfillment, and Service Request Fulfillment) defined in **Exhibit 3.1 Service Level Matrix** and **Exhibit 3.2 Service Level Definitions.** The outcomes of the Request Management and Fulfillment processes will be measured by the Shared Service Growth Key Performance Indicator and the Customer Satisfaction Key Performance Indicator defined in **Exhibit 3.4 Performance Analytics.** The DIR Customer's Monthly Scorecard of the Successful Respondent's performance will indicate whether the Successful Respondent is meeting the DIR Customer's service needs, as defined in **Exhibit 3.5 Customer Satisfaction.** The availability of Request Management systems will be measured by the Critical SLA "MSI Shared Services Systems Availability," defined in **Exhibit 3.1 Service Level Matrix** and **Exhibit 3.2 Service Level Definitions**

3.5.1 Request Management System

The Successful Respondent shall deploy and utilize a Request Management System that provides a level of sophistication to promote the fulfillment of Service Requests associated with the Services within designated timeframes that accurately prioritizes and coordinates fulfillment efforts according to the business need of DIR and DIR Customers, and generally promotes good customer service and expectation setting.

The Successful Respondent's shall, at a minimum:

3.5.1.1 Implement an automated Request Management System, including the integration of applicable software, equipment, email, telephony, and Web technologies.

Exhibit 2.1 Statement of Work　　　　　　　　　　　　　　　　　　　　　　　Page 45

3.5.1.2   Receive and record all Service Requests (including submissions received by telephone, chat, Service Catalog, electronically, or other means approved by DIR) in a Service Request Record, including classification and initial support.

3.5.1.3   Utilize and update the Request Management System with all relevant information relating to a Service Request.

3.5.1.4   Validate that the Request Management system contains the solution and proposed cost for each Service Request, with the appropriate authorized DIR Customer approval of the Service Request, and the link to invoicing for that service.

3.5.1.5   Facilitate and lead the design and provide workflow and interface capabilities to:

    3.5.1.5.1   Facilitate and lead the automation and orchestration of Service Requests between the Successful Respondent and SCP(s).

    3.5.1.5.2   Facilitate and lead the design and provide workflow and interface capabilities to enable the SCPs to initiate fully automated and orchestrated request fulfillment.

    3.5.1.5.3   Automate password Service Requests from the Service Catalog to the Successful Respondent and SCP(s) systems.

    3.5.1.5.4   Integrate with other Request Management systems of other SCPs as directed by DIR.

    3.5.1.5.5   Provide customizable capability that allows different configurations of interfaces based on standard user profiles.

    3.5.1.5.6   Provide workflow and interface capabilities to enable the SCPs to initiate fully automated and orchestrated request fulfillment.

3.5.1.6   At a minimum, the Request Management System shall:

    3.5.1.6.1   Securely segregate DIR and DIR Customer data so that it can be accessed only by those authorized to comply with Government security requirements and in accordance with DIR policy.

    3.5.1.6.2   Provide for the partitioning of DIR Customer information in management and reporting.

    3.5.1.6.3   Provide for granting additional access in support of other Authorized Users (e.g., Audits) as directed by DIR.

    3.5.1.6.4   Provide automated workflow and interface capabilities to connect SCPs and coordinate fully automated and orchestrated request fulfillment.

    3.5.1.6.5   Provide information necessary to record, track, and support Request Management as defined in the DIR-approved SMM for each Service Request submitted.

    3.5.1.6.6   Provide for logging all modifications to Service Request records, to provide full tracking, audit trail and change control at the named-user level.

    3.5.1.6.7   Provide functionality to manage information for each Service Request submitted to, and originating from, Successful Respondent.

Exhibit 2.1 Statement of Work   Page 46

3.5.1.6.8 Link multiple contacts pertaining to the same Service Request to the associated Service Request record.

3.5.1.6.9 When multiple Service Requests pertain to the same essential work, link the multiple Service Request records to a single Service Request.

3.5.1.6.10 Provide online reporting capability with real-time visibility of data records associated with Service Requests (and with unrestricted query length and depth) for use by Authorized Users in the generation of sophisticated, custom reports.

3.5.1.6.11 Provide end-to-end traceability, even when transactions span across multiple Applications, systems components, or parties.

3.5.1.7 Develop, utilize, manage and continually improve an inventory of defined and documented Service Request models that incorporate at a minimum the following elements:

3.5.1.7.1 Sequences of tasks, actions or steps to execute the Service Request Model and fulfill the Service Request.

3.5.1.7.2 Identification of required dependencies, data sources, etc., that must be considered in executing the Service Request Model.

3.5.1.7.3 Definition of responsibilities and roles to execute the Service Request Model.

3.5.1.7.4 Timescales, milestones and thresholds for executing the Service Request Model.

3.5.1.7.5 Anticipated escalation points and escalation procedures associated with the Service Request Model.

3.5.2 Request Management Process

The Successful Respondent shall, at a minimum:

3.5.2.1 Develop and document in the Service Management Manual Request Management processes and procedures regarding interfaces, interaction, and responsibilities between Level 1 Support personnel, Level 2 Support personnel, and any other internal or external persons or entities that may support the fulfillment of Service Requests, subject to DIR approval.

3.5.2.2 Provide a mechanism for handling of Service Requests according to the agreed to prioritization model used by DIR, DIR Customers, and SCP(s) as per processes described in the DIR-approved SMM, and in keeping with the appropriate SLAs.

3.5.2.3 Provide a mechanism for expedited handling of Service Requests that are of high business priority to DIR, DIR Customers, and SCP(s) based on the assigned priority, as per escalation processes and procedures described in the DIR-approved SMM.

3.5.2.4 Provide a mechanism for escalation of Service Requests that have missed or are at risk of missing expectations (e.g., fulfilment date, request scope, or other commitments), as per processes described in the DIR-approved SMM.

Exhibit 2.1 Statement of Work   Page 47

3.5.2.5 Provide criteria and establish processes to support the proper procedure for requesting the expedited handling of Service Requests.

3.5.2.6 Provide criteria and establish processes for DIR, DIR Customers, and designated Third Party Vendor(s) to escalate Service Requests.

3.5.2.7 Establish processes that properly route Service Requests across the Successful Respondent and multiple SCPs and organizations.

3.5.2.8 Develop and establish guidelines for closure where Authorized User's confirmation has not been received.

3.5.3 Request Management Operations for All Service Requests

For all Service Requests including those worked by SCPs and those worked by the Successful Respondent, the Successful Respondent shall, at a minimum:

3.5.3.1 Provide a process to coordinate Request Management activities across all SCPs, DIR Customers, and DIR.

3.5.3.2 Escalate a Service Request where the Service Request cannot be completed within the relevant Service Levels or agreed timeframe, in accordance with the relevant DIR-approved SMM.

3.5.3.3 Ensure all appropriate parties are notified of the SLA allotted resolution time for each Service Request and provide automated triggers to escalate a Service Request nearing the allotted resolution time.

3.5.3.4 Lead the effective execution of automated Request Management processing, including:

    3.5.3.4.1 Manage the effective execution of automated Request Management to achieve its primary purpose to fulfill Service Requests within the agreed Service Levels and promote DIR Customer and Authorized User satisfaction.

    3.5.3.4.2 Provide for mechanisms to support automated ordering and billing to other SCPs and designated Third Party Vendors, for Service Requests associated with the delivery of Services and where authorized by DIR or DIR Customers.

    3.5.3.4.3 Ensure that detailed audit trail information be recorded of all activity that creates, changes, or deletes data and user access to systems that contain DIR and DIR Customer data.

    3.5.3.4.4 End-to-end traceability must be provided even when transactions span across multiple Applications, systems components, or parties.

3.5.3.5 Provide effective Service Request Governance to ensure the following:

    3.5.3.5.1 Establish on-going working relationship with the Service Component Providers, DIR, and DIR Customers for effective Service Request governance and the overall effective execution of the Request Management processes across the Successful Respondent and all SCPs, and in compliance with the Governance provisions of this agreement.

Exhibit 2.1 Statement of Work   Page 48

3.5.3.5.2 Clearly define and document the type of Service Requests that will be handled within the Request Management process so that all parties are absolutely clear on the scope of Service Requests and the Request Management process.

3.5.3.5.3 Establish and continually maintain definitions of all Services, including descriptions, what Services will be standardized, what Services require a custom solution, and what Services and components can be requested through each medium (e.g., Service Desk, Portal, Service Catalog, RFS, etc.).

3.5.3.5.4 Maintain current service definitions on the Portal's Service Offerings for DIR Customers.

3.5.3.6 Facilitate the SCPs' progression to standardize Services with the objective to provide self-provisioning of all Services, leveraging automation and orchestration to accelerate the order and fulfillment process.

3.5.3.6.1 Establish and continually maintain Authorized Users lists on who is authorized to make Service Requests and what requests they are entitled to make.

3.5.3.6.2 Communicate to DIR and DIR Customers on the definition of services, the Request Management processes, and changes thereto.

3.5.3.6.3 Regularly collect feedback from Authorized Users on the effectiveness of Request Management, and engage in activities for improvement.

3.5.3.7 Ensure proper approval (including any financial costs) associated with the Service Request (through automated means where practical) prior to Service Request fulfillment.

3.5.3.8 Ensure that Service Requests follow the Change Management process as appropriate.

3.5.3.9 Review and analyze Service Request trends to identify opportunities for service enhancements (e.g., opportunities for self-provisioning, automation, New Services, etc.). Propose enhancements to DIR and SCPs, and implement if approved.

3.5.4 Request Management Operations for Requests the Successful Respondent Owns

For Service Requests that span multiple SCPs thereby requiring facilitation, the Successful Respondent is responsible for owning the end-to-end resolution. The Successful Respondent shall, at a minimum:

3.5.4.1 For Service Requests spanning multiple SCPs, provide a process for the end-to-end Service Request coordination, thus minimizing redundant contacts with the Authorized User.

3.5.4.2 Update required information on Service Requests within timeframes defined in the SMM to support an up-to-date accurate view of Service Requests.

3.5.4.3 Ensure proper approval (including any financial costs) associated with the Service Request (through automated means where practical) prior to Service Request fulfillment.

Exhibit 2.1 Statement of Work   Page 49

3.5.4.4   Provide and maintain regular communications between all parties and Authorized Users as required until Service Request completion and document the communications as per the Request Management processes.

3.5.4.5   Keep DIR and DIR Customers informed of any issues with the completion of Service Requests and status changes throughout the Service Request life cycle and in accordance with agreed Service Levels defined in **Exhibit 3.1 Service Levels Matrix**.

3.5.4.6   Determine the frequency of such communications by the severity of the Service Request and in compliance with Service Request policies and procedures in the DIR-approved SMM.

3.5.4.7   Provide anticipated completion times for active Service Requests and update notification systems as required in the Request Management processes to keep Customers and Authorized Users informed in accordance with established Service Levels per **Exhibit 3.1, Service Level Matrix** and **Exhibit 3.2, Service Level Definitions**.

3.5.4.8   Ensure ownership of Service Requests from creation to completion.

3.5.4.9   Close Service Requests, per DIR-approved SMM, after receiving confirmation from the requesting Authorized User or SCP support personnel that the Service Request has been completed.

3.5.4.10 Track the progress of fulfillment efforts and the status of all Service Requests per the DIR-approved SMM, including:

   3.5.4.10.1 Communicate the proposed fulfillment time for each Service Request with the appropriate party and update the status accordingly.
   3.5.4.10.2 Provide regular updates as to the status of all Service Requests within designated SLA timeframes.
   3.5.4.10.3 Coordinate Service Request tracking efforts with the SCPs, and provide and maintain regular communications, per the DIR-approved SMM, between all parties and Authorized Users until Service Request completion.
   3.5.4.10.4 Keep the DIR Customer and Authorized User informed of changes in Service Request status throughout the Service Request life cycle in accordance with agreed Service Levels.
   3.5.4.10.5 Keep DIR Customer informed of anticipated Service Request completion times for active Service Requests.
   3.5.4.10.6 When a Service Request cannot be completed in the committed timeframe, provide for a revised completion time in alignment with established SMM process.
   3.5.4.10.7 Track all Service Request completions against the target timeframes.

3.5.4.11 Utilize the Successful Respondent Request Management System for all Request Management and Fulfillment activities.

Exhibit 2.1 Statement of Work   Page 50

3.5.4.12 Provide for timely receipt and processing of all requests within designated timeframes from the Request Management System.

3.5.4.13 Utilize and update the Request Management System with all relevant information relating to a Service Request.

3.5.5 Request for Solution (RFS)

Requests for Solution (RFS) are those types of DIR Customer requests where requirements are captured in the Successful Respondent's Request Management system and SCP's develop solutions and cost estimates for DIR Customer review and approval. These solutions typically assume the SCP builds and implements the solution.

The timeliness and effectiveness of the Request for Solution process will be measured by Key SLAs (Solution Proposal and Solution Implementation) defined in **Exhibit 3.1 Service Level Matrix** and **Exhibit 3.2 Service Level Definitions.** Customer satisfaction with the Successful Respondents performance will be measured in the Monthly Customer Scorecard, defined in **Exhibit 3.5, Customer Satisfaction.**

For DIR Customer Requests which require an SCP to propose a solution, the Successful Respondent's shall, at a minimum:

3.5.5.1 Lead SCPs in developing and establishing RFS processes and appropriate mechanisms for the electronic capture and fulfillment of complex requests requiring design, price (e.g., electronic Cost Estimating Tool (CET)), solution, and proposals; including appropriate communications to adequately set expectations and promote good customer service.

3.5.5.2 Lead the process across all SCPs to develop and establish RFS processes and appropriate mechanisms to support rapid proposal development that provides a level of accuracy for budgetary information without requiring a full solution (e.g., Rough Order Magnitude (ROM) pricing and high level architecture).

3.5.5.3 For all RFS projects:

   3.5.5.3.1 Provide project administration oversight throughout the RFS lifecycle as defined in the DIR-approved SMM.
   3.5.5.3.2 Monitor to ensure each step of the RFS Lifecycle is achieved and documented in accordance with established procedures as per the DIR-approved SMM.
   3.5.5.3.3 Monitor the RFS-related Service Level performance and implement corrective action as needed to achieve the targeted Service Level performance.
   3.5.5.3.4 Monitor to ensure successful final project closure.

3.6   Change Management

Change Management comprises an end-to-end solution that minimizes risk, cost, and business disruption, while protecting the computing and the delivery of related Services. All changes to Configuration Items must be carried out in a planned and authorized manner. This includes identifying the specific Configuration Items and IT Services affected by the Change, planning

Exhibit 2.1 Statement of Work   Page 51

the Change, communicating the Change, deploying the Change, testing the Change, and having a back-out plan should the Change result in a disruption of the Service. This also includes tracking and oversight for all Changes.

The effectiveness of the Change Management process will be measured by Key SLAs (Change Management Effectiveness) defined in **Exhibit 3.1 Service Levels Matrix** and **Exhibit 3.2 Service Level Definitions**, as well as through Key Performance Indicators defined in **Exhibit 3.4, Performance Analytics.** Customer satisfaction with the Change Management process will be measured in the Monthly Customer Scorecard, defined in **Exhibit 3.5, Customer Satisfaction.** The availability of Change Management systems will be measured by the Critical SLA "MSI Shared Services Systems Availability," defined in **Exhibit 3.1 Service Level Matrix** and **Exhibit 3.2 Service Level Definitions**

3.6.1 Change Management System and Process

The Successful Respondent shall, at a minimum:

3.6.1.1 Maintain the processes as defined in the SMM and approved by DIR. Evaluate processes for improvement opportunities, recommend changes to DIR and implement approved changes.

3.6.1.2 Maintain and routinely improve the use of Change Models for repetitive Changes to improve the efficiency and effectiveness of the Change process.

3.6.1.3 Deploy and maintain workflow-based tools to automate the process of recording, assessing, scheduling, documenting, authorizing, tracking, and reporting on Changes.

3.6.1.4 Deploy and maintain tools and processes to enable the Digital CAB where changes are initiated through the Service Catalog and routed through automated workflow to all participants requiring review, feedback, approval and scheduling.

3.6.1.5 Deploy and maintain tools and processes to support an efficient integrated CAB report which contains all changes, both digitally reviewed and those going through a traditional CAB.

3.6.1.6 Provide capability for logging all modifications to Change Records, to provide full tracking, audit trail and change control at the named-user level.

3.6.2 Change Management Maintenance Periods

The Successful Respondent shall, at a minimum:

3.6.2.1 Establish and document standard periods for maintenance in the SMM.

    3.6.2.1.1 Establish periods for routine and regular maintenance for DIR Shared Technology Services under Successful Respondent management.

    3.6.2.1.2 Establish specific periods for Enterprise maintenance impacting multiple organizations (e.g., shared infrastructure).

      3.6.2.1.3 Establish processes for scheduling and getting approval of other maintenance (e.g., urgent but non-emergency).

      3.6.2.1.4 Establish processes for coordinating and planning maintenance periods with Customers and Service Component Providers as appropriate.

      3.6.2.1.5 Establish communications plans to support maintenance and appropriately inform SCPs, DIR, and DIR Customers.

3.6.2.2 Regularly communicate and re-communicate, as necessary, the established maintenance periods with SCPs, DIR, and DIR Customers, and as necessary communicate when any time maintenance periods are revised.

3.6.2.3 Perform maintenance during regular Maintenance Periods as defined in the SMM, or as scheduled in advance with the approval of DIR or DIR Customers.

3.6.2.4 Actively manage changes such that systems are down for a minimum amount of time..

3.6.2.5 Provide appropriate notice to DIR and DIR Customers of the maintenance to be performed during scheduled maintenance windows, based on the categorized risk of the Change and as specified in the SMM.

3.6.2.6 Schedule Outages for maintenance, expansions, and modifications during hours that meet DIR's and DIR Customers' business needs.

3.6.2.7 Stagger maintenance as appropriate to accomplish all work across all DIR Customers within the establish time-frames and based on the categorized risk of the Change.

3.6.2.8 Allow DIR and DIR Customers, as described in the SMM, to specify "freeze" periods during which Successful Respondent and SCPs will not make any Changes.

3.6.2.9 If there is a need for emergency systems maintenance, provide SCPs, DIR, and DIR Customers with as much notice as reasonably practicable, and perform such maintenance so as to minimize interference with the business and operational needs of DIR and DIR Customers.

3.6.2.10 Identify when change management procedures or policies have not been followed and direct associated and appropriate parties to establish plans for correcting.

3.6.2.11 Coordinate the establishment and routine update of maintenance periods for Successful Respondent and other SCPs, which support both the regular and normal maintenance of the Infrastructure and Services while protecting DIR and DIR Customers from unplanned outages.

3.6.2.12 Routinely maintain a current projected service outage document (in conjunction with the Availability Management process) which defines scheduled service outages, for both regularly scheduled maintenance outages and other scheduled outages, provide the document, and report on projected service outages to DIR and DIR Customers as required.

3.6.3   Change Management Operations

The Successful Respondent shall, at a minimum:

3.6.3.1   Coordinate and execute Change Management activities for DIR Shared Technology Services across all DIR Customers, DIR, and SCPs that provide services to DIR Customers.

3.6.3.2   Establish the operation and composition of each CAB and Emergency Change Advisory Board for DIR Shared Technology Services and DIR Customers, including membership, practices, tools (e.g., action lists, electronic meeting facilities, recording of approvals, etc.), agendas, cadence, etc.

3.6.3.3   Within the Change Management Process, define the types of changes eligible for review, approval, and scheduling by way of a digital CAB whereas the change is routed through Successful Respondent-provided workflow to all participants requiring review, feedback, approval, and scheduling.

3.6.3.4   Prepare CAB information, schedule, participate, and lead regularly scheduled CAB meetings with DIR, DIR Customers, and SCPs according to the approved Change Management process.

3.6.3.5   Where a proposed Change represents a potentially high risk or high impact to Customers' operations or business, or at the request of DIR Customer, Successful Respondent shall work with the change owner (e.g., SCP) to attach a comprehensive end-to-end test plan (including clear Change acceptance criteria), notification and escalation lists, and work-around plans to the Change.

3.6.3.6   The concept of comprehensiveness should apply consistently across risk levels and whether the change planning is for a DIR Customer change or an enterprise change; a comprehensive plan should include at least the following:

   3.6.3.6.1   A full description of the change, including the purpose of the change.
   3.6.3.6.2   Pre-Installation planning (where possible includes demonstrating testing in non-production environments).
   3.6.3.6.3   Communication planning (Includes communications throughout the lifecycle of the change).
   3.6.3.6.4   Installation planning.
   3.6.3.6.5   Post-Installation planning (includes testing and validation).
   3.6.3.6.6   Impact analysis (impact of performing and not performing the change).
   3.6.3.6.7   Complete planning with cross-Service Component entities.
   3.6.3.6.8   Include a comprehensive contingency plan, including a back-out plan and procedures (with specific criteria as to when to initiate the execution of the back-out plan).

3.6.3.7   For changes authorized for Digital CAB:

Exhibit 2.1 Statement of Work   Page 54

3.6.3.7.1 Facilitate electronic CABs by preparing and routing Changes through workflow to the appropriate reviewer and approver.

3.6.3.7.2 Review proposed Changes and schedules in compliance with the approved Change Management process.

3.6.3.8 For changes not authorized for Digital CAB:

3.6.3.8.1 Conduct regularly CAB meetings at the enterprise and DIR Customer level to review and approve proposed Changes.

3.6.3.8.2 Where possible, the CABs will be electronically administered through the Digital CAB workflow so as to avoid separate meetings for each DIR Customer each week.

3.6.3.8.3 Large DIR Customers with complex changes and the Enterprise-wide CAB each may require a CAB meeting each week where changes are reviewed using the Digital CAB dashboard for efficiency.

3.6.3.9 For all Changes, electronically capture and publish integrated Change Management status reports to all relevant stakeholders, including DIR, DIR Customers, other SCPs, and authorized Third Party Vendors.

3.6.3.10 Verify that all Requests for Change (RFC) are done through the appropriate method, meet the appropriate criteria, and follow the approved process, as defined in the DIR-approved SMM.

3.6.3.11 Provide a standard electronic RFC form that will be used to request Changes and that will remain in use throughout the life of the change until formal closure as called for by the Change Management Process.

3.6.3.12 Reject or return to the Requestor those RFCs which do not meet the minimum change criteria as defined in the DIR-approved SMM.

3.6.3.13 Summarize the Changes made and attempted each week, and report the information to DIR and DIR Customers on a weekly basis.

3.6.3.14 Capture all DIR Customer Change data centrally, and make it available to DIR, DIR Customers, and Authorized Users.

3.6.3.15 Establish a single focal point for changes to minimize the probability of conflicting changes and potential disruption to the production environments.

3.6.3.16 Defining change windows and black-out periods, including the enforcement and authorization for exceptions.

3.6.3.17 Conduct Post Implementation Reviews (PIR) on Changes as requested by DIR.

3.6.3.18 Provide a change categorization schema, subject to DIR approval, that will be used to categorize all changes.

Exhibit 2.1 Statement of Work   Page 55

3.6.3.19 Provide a change prioritization schema, subject to DIR approval, that will be used to prioritize changes.

3.6.3.20 Report to DIR and DIR Customers on change activity in the Enterprise that presents high risk and propose actions to address.

3.6.3.21 Review proposed Changes and schedules, testing, implementation plans, back out, and remediation plans for every RFC as part of the information used for change approval.

3.6.3.22 Provide a regularly updated and reported Change Schedule that includes details of all scheduled changes.

3.6.3.23 Ensure that the Asset Inventory Management System and Configuration Management System is updated throughout the process.

3.6.3.24 Report the status of scheduled Changes, including maintaining a comprehensive list of projects and dates to affected DIR Customers and SCPs.

3.6.3.25 Provide information to DIR, DIR Customers, and SCPs in accordance with the Change Management process on the outcome of any RFC and the updated status after each Change is implemented. Collect data on every Change attempted, which includes the following:

    3.6.3.25.1 Include the cause of any Incidents, measures taken to prevent recurrence, and whether the Change was successful from the perspective of the Authorized User or SCP affected by the Change.
    3.6.3.25.2 Summarize and report this data to DIR on a periodic basis as describe in **Attachment 3.4A Reports**.

3.6.3.26 Provide an audit trail of any and all Changes to all environments, which should include a record of the Change made and the authorization to make the Change.

3.6.3.27 Conduct Post Implementation Reviews (PIR) on Changes, if requested by DIR or Customer.

3.6.3.28 Provide DIR with the ability to pre-approve certain types of routine operational Changes (Standard Changes). Such approvals shall be documented in the SMM.

3.6.3.29 Verify that the effective execution of the Change Management Process, as well as an appropriate review of planned changes, takes place with due consideration of the business and technology risk of planned changes, and all defined criteria (such as complexity of change, the skill level of the individual(s) executing the change, the planned change execution timeframe, the change slot timeframe, the back-out timeframe, pre-change technical deployment planning, communication planning, post-change validation planning, and the relevant business processing criticality).

3.6.3.30 With proper authorization, stop any planned changes that would compromise the continuation of Services to DIR and DIR Customers, and act as the gatekeeper to

Exhibit 2.1 Statement of Work   Page 56

production, unless expressly overridden by the DIR Operations Manager in accordance with the approved Change Management escalation process.

3.6.3.31 Assume responsibility for escalating and ensuring parties responsible for resolution are properly engaged for any issues arising from the decision to stop a planned change.

3.6.3.32 Monitor change closure status for appropriate success/failure classification.

3.6.3.33 Conduct joint review of any change failures with SCPs, and provide a strong interlock between change and Incident Management and Problem Management processes so that post-change issues can be linked to the change activity where relevant.

3.6.3.34 Continuously work with Successful Respondent staff to understand success/failure criteria and integration requirement with Incident and Problem Management.

3.6.3.35 Manage to Resolution any SCP deviation from effective Change Management Process, ensuring the review and closure of failed changes.

3.6.3.36 Monitor and report progress, issues, and status related to Change implementation to all relevant parties.

3.6.3.37 Provide a documented list of Standard Changes in appropriate DIR and DIR Customer documents which are pre-approved changes for a specific, low-risk change that has a defined Change Model and a defined set of processes and procedures.

3.6.3.38 Identify opportunities for non-standard changes to be defined and classified as Standard Changes to improve overall Change Management efficiency. Implement those opportunities with the SCPs.

3.6.3.39 Review all changes in terms of the following:

> 3.6.3.39.1 Success or failure (based on the established criteria for change success or failure established in the policies and procedures for the Change Management process or the Change).
>
> 3.6.3.39.2 Operational soundness of the services offered to DIR and DIR Customers and the technical systems and components that support them following the change.
>
> 3.6.3.39.3 Proper completion of all required change documentation (based on the established policies and procedures for the Change Management process).

3.6.3.40 Close all Changes following a review of each Change with other SCPs and DIR Customers.

3.7   Asset Inventory and Management

3.7.1   Asset Inventory and Management System

The Successful Respondent shall, at a minimum, develop, implement, and maintain automated Asset Inventory and Management System (AIMS) tools for all Services and Successful Respondent-provided processes. The quality and effectiveness of the Asset Inventory and

Exhibit 2.1 Statement of Work   Page 57

Management system and processes will be measured by Critical SLAs (Data Quality) defined in **Exhibit 3.1 Service Level Matrix** and **Exhibit 3.2 Service Level Definitions.** The effectiveness of automation will be measured by the Critical Deliverable CMDB and Data Quality Management Automation defined in **Exhibit 3.3, Critical Deliverables.** The availability of Asset Inventory Management systems will be measured by the Critical SLA "MSI Shared Services Systems Availability," defined in **Exhibit 3.1 Service Level Matrix** and **Exhibit 3.2 Service Level Definitions**

The Successful Respondent shall provide automated tools and processes that:

3.7.1.1   Provide, operate and manage electronic Data Quality Management (DQM) capabilities and processes to execute ongoing inventory reconciliation activities which take in multiple asset inventory sources (e.g., industry hardware and software catalogs, electronic discovery, monitoring, active directory, the Successful Respondent and SCPs, and Third Party Vendor systems and inventories) from the Successful Respondent and SCPs and Third Party Vendors and electronically correlate and automatically identify, reconcile Equipment, Software, and related IT services in the AIMS database.

3.7.1.2   Ensure effective deployment and re-use of DIR, DIR Customer, and Successful Respondent-owned technology assets.

3.7.1.3   Enable a common view in terms of information access and presentation by DIR, DIR Customers, the Successful Respondent, and SCPs.

3.7.2   Asset Inventory and Management Operations

The Successful Respondent shall, at a minimum:

3.7.2.1   Using DQM capabilities, conduct an initial, complete electronic inventory of all Equipment, Software, and related services provided or supported by Successful Respondent and deployed at DIR and DIR Customers' Sites or SCP locations. This initial inventory will include all IT assets, whether such assets are owned or leased by DIR, DIR Customers, or SCPs.

3.7.2.2   Schedule and manage to completion this initial inventory in accordance with the CMDB Data Quality and Automation Critical Deliverable as listed in **Exhibit 3.3 Critical Deliverables**.

3.7.2.3   Record, at a minimum, the individual data elements for each asset as part of the initial inventory as specified in the SMM and as applicable for individual asset types.

3.7.2.4   As the initial asset inventory is being conducted, enter the required information regarding the assets into Successful Respondent's AIMS.

3.7.2.5   DIR will approve the AIMS and the initial inventory before final implementation.

3.7.2.6   Provide processes and tools to ensure the AIMS is continuously updated, and at a minimum, accomplish the following:

Exhibit 2.1 Statement of Work   Page 58

3.7.2.6.1 Remove assets that are no longer in use, in accordance with DIR policies.

3.7.2.6.2 Modify asset information resulting from asset relocation and/or use by a different Authorized User.

3.7.2.6.3 Modify asset information due to upgrades and Software updates.

3.7.2.6.4 Add new asset information upon implementation of new Equipment or Software.

3.7.2.7 Where Equipment has been identified by DIR and DIR Customer as co-located, Successful Respondent will track those items and ensure they are exempted from receipt of the applicable Services, as specified in the SMM.

3.7.3 Site Information Management

The Successful Respondent shall, at a minimum:

3.7.3.1 Maintain a comprehensive and master listing of DIR and DIR Customer Sites receiving Services.

3.7.3.2 Provide access to the master list to DIR, DIR Customers, and SCPs. Regularly provide complete Site Information to DIR, DIR Customers, and SCPs as specified by DIR.

3.7.3.3 Provide for and maintain meaningful cross-references to site nomenclature and identifiers within DIR's, DIR Customers', and SCPs' systems as specified by DIR.

3.7.3.4 Ensure that Site Information is accurately maintained and distributed to support the delivery of Services, and in a manner consistent with all of Configuration Management.

3.7.3.5 Ensure that all Successful Respondent Shared Services Systems, FAQs, documents, training material and other relevant areas are regularly updated with Site Information.

3.7.3.6 Provide electronic, Service Catalog-driven processes for DIR, DIR Customers, and SCPs to request changes to the Site Information. The Successful Respondent shall document and maintain processes within the SMM, subject to DIR approval.

3.7.3.7 Provide updates based on DIR and DIR Customer change requests within designated timeframes.

3.7.3.8 Document and escalate to DIR where SCPs or DIR Customers are not accurately or updating Site Information within designated timeframes.

3.8   Software License Management

3.8.1 Software License Renewal Management

The Successful Respondent has responsibility for tracking, monitoring, and reporting the software renewal process to ensure compliance with agreements and continued operation in the environment across all Shared Services and SCPs.

Exhibit 2.1 Statement of Work   Page 59

The effectiveness of Software License Renewal Management will be measured by the Key SLA License and Maintenance Timeliness, defined in **Exhibit 3.1 Service Level Matrix** and **Exhibit 3.2 Service Level Definitions.** The availability of Software License Management systems will be measured by the Critical SLA "MSI Shared Services Systems Availability," defined in **Exhibit 3.1 Service Level Matrix** and **Exhibit 3.2 Service Level Definitions**

The Successful Respondent shall, at a minimum:

3.8.1.1   Continually verify the Successful Respondent's and SCPs' effective compliance with the Software License Renewal Management processes, as defined in the SMM.

3.8.1.2   Coordinate Software License Renewal Management activities across all functions and SCPs that provide services to DIR Customers.

3.8.1.3   Initiate and manage the overall Software License Renewal Management process with the SCPs to meet the schedule and business needs of the DIR and DIR Customers.

3.8.1.4   Answer questions and provide research as needed to DIR, DIR Customers, and SCPs, with respect to the Software License Renewal System and Change Management System.

3.8.1.5   Providing weekly status reporting to DIR, DIR Customers, and SCPs as needed and defined in the SMM.

3.8.1.6   Initiate Requests and Change Requests as appropriate for all renewals and ensure updates reflect the status of each renewal as per the timing and lifecycle process defined in the SMM. (e.g., Software expiring in May should be logged as a CRQ in January which is one hundred twenty (120) days prior to the Expiration date).

> **NOTE**: SCPs will perform the role of updating the contract data in the approved Software License Renewal System, coordinating with the DIR Customer, the Successful Respondent, and SCP(s) to obtain renewal approvals, execute the procurement tasks to renew the software license, install the renewed keys and software, and updating the Change Request and Contracts data, and log the renewed software keys in the Software License Renewal System as per the process defined in the SMM.

3.8.1.7   Monitor Software License Renewal progress and SLA achievement.

3.8.1.8   Ensure the requests and Change Requests are completed and closed upon renewal completion.

3.8.2   Software License Compliance Management

The Successful Respondent shall determine the compliance position, monitor, and report on the software compliance management process to ensure compliance with agreements and reduce operating risk in the environment.

Exhibit 2.1 Statement of Work   Page 60

The effectiveness of Software License Compliance Management will be measured by the Critical SLA Software License Compliance Position Reporting, defined in **Exhibit 3.1 Service Level Matrix** and **Exhibit 3.2 Service Level Definitions.**

The Successful Respondent shall, at a minimum:

3.8.2.1 Continually verify the Successful Respondent's and SCPs' effective compliance with the Software License Compliance Management Policies as documented in the SMM.

3.8.2.2 Coordinate and manage Software License Compliance Management activities across all SCPs that provide services to DIR Customers regardless of which entity has financial responsibility for the Software (e.g., security, certificates).

    3.8.2.2.1 Provide system and process for SCPs and DIR Customers to collect, and maintain Proof of Entitlement (POE) data.

    3.8.2.2.2 Coordinate with the SCPs in their collection of POE data, track and report on collection status.

    3.8.2.2.3 Coordinate SCPs to collect and normalize software titles to standard names, and maintain in a system, the software titles deployed in the environment.

    3.8.2.2.4 Generate, publish, and review the Software License Compliance position for DIR and DIR Customers, and determine appropriate remediation.

    3.8.2.2.5 Upon DIR request, generate and report the Software License Compliance position for SCPs.

    3.8.2.2.6 For DIR and DIR Customer remediation items, initiate and coordinate actions through the Incident, Request, Change, and Project processes for any reported non-compliance of software purchased versus software installed.

    3.8.2.2.7 For DIR and DIR Customer remediation items, provide clarifications about information presented in the Compliance Report to eliminate discrepancies found.

3.8.2.3 Proactively manage the use of the Software within the DIR Shared Technology Services environment in order to maintain strict compliance, including but not limited to:

    3.8.2.3.1 Immediately notify and advise DIR of all Software license compliance issues associated with DIR Shared Technology Services.

    3.8.2.3.2 Obtain, track and maintain the applicable licensing and use information received from DIR Customers.

    3.8.2.3.3 Report on Equipment with the presence of any unauthorized or non-standard Software.

    3.8.2.3.4 Track and report licenses and license counts and association with any DIR Shared Technology Services Configuration Item (CI) that is within the CMDB.

    3.8.2.3.5 Manage and track security certificates used to secure confidential sessions (e.g., SSL) for Internet and Intranet transactions and communications, including processes and procedures for renewals, as required by DIR or DIR Customers.

Exhibit 2.1 Statement of Work   Page 61

3.8.2.4   Confirm the presence and version of Software installed on a particular device and that those attributes are recorded in the asset management system.

3.8.2.5   Provide reporting of license information and compliance to DIR, at least quarterly or as directed by DIR.

3.9   Configuration Management

Configuration Management will provide a logical model of the IT infrastructure by identifying, controlling, maintaining, and verifying information related to all CIs that support the services offered to DIR and DIR's Customers.

Configuration Management will include the implementation of a Configuration Management System (CMS), incorporating information from multiple databases (Configuration Management Databases – CMDBs) and containing details of the components or CIs that are used in the provision, support and management of DIR Shared Technology Services across all Service Component Providers. The CMS will contain information that relates to the maintenance, movement, and problems experienced with the CI, and their relationships.

Application Portfolio Management (APM) is an optional service for DIR Customers that is being developed. APM provides a centralized approach for collecting, analyzing and describing a DIR Customer's business applications thereby allowing them to make informed, prioritized investment and risk decisions in technology services that support their business needs. While the APM capability is being developed as a stand-alone service, the MSI provided Configuration Management System (CMS) shall provide a container to store select APM attribution (e.g., Business Application names) for DIR Customers as required to efficiently share data between the CMS and the APM service. The APM service will provide the single repository of truth for DIR Customer business application data.

The effectiveness of Configuration Management and APM will be measured by Critical SLAs (Resolution time, Data Quality - Enterprise) and Key SLAs (Change Management Effectiveness) defined in **Exhibit 3.1 Service Level Matrix** and **Exhibit 3.2 Service Level Definitions.** The availability of the Configuration Management Systems and APM Systems will be measured by the Critical SLA "MSI Shared Services Systems Availability," defined in **Exhibit 3.1 Service Level Matrix** and **Exhibit 3.2 Service Level Definitions**

3.9.1   Configuration Management System and Processes

The Successful Respondent shall, at a minimum:

3.9.1.1   Implement a Configuration Management System (CMS) system which incorporates information from multiple databases (CMDBs) and data sources, and contains the single source for CI details that are used in the provision, support and management of DIR Shared Technology Services.

3.9.1.2   Integrate the Configuration Management processes and data of DIR and SCPs, with the Successful Respondent's Configuration Management processes where the processes interact; including providing Configuration data electronically to the CMS.

3.9.1.3   Create and maintain an automated Configuration Management Validation Plan, agreed

Exhibit 2.1 Statement of Work   Page 62

to by DIR, that continually performs electronic logical validation of all equipment, software, applications and relationships provided by the SCP(s) with the CMS.

    3.9.1.3.1 Provide logical validation of all CIs from the SCP(s) to the CMS and from CMS to the SCP(s).

    3.9.1.3.2 Continually verify the effective execution of the automated Configuration Management Validation Plan, by Successful Respondent and SCPs.

    3.9.1.3.3 Reconcile to APM-provided master product lists (e.g., industry product lists for software, hardware, cloud services) for use in identifying non-reference CIs, thereby providing reference architecture governance. This may be in addition to any industry lists provided by the Successful Respondent to perform other requirements (e.g., Software License Compliance).

    3.9.1.3.4 For equipment where data sources are not available, the Successful Respondent shall include approved exceptions to perform electronic logical validations.

3.9.1.4 Implement and maintain a Data Quality Management System to enable an automated CMS data normalization and reconciliation process. This process will support the automated Configuration Management Validation Plan by leveraging electronically discovered and enriched data provided from the Service Component Providers and Customers.

3.9.1.5 Grant DIR and Customers access to the CMS, and allow DIR to monitor and view on an ongoing basis. For Customers that only receive APM services, access to the CMS is not required.

3.9.1.6 Make the complete CI dataset, including resource information, service information, cost information and application information (with associated relationships), available to the APM service through an agreed upon interface (e.g. direct database, replicated database, Web Services interface, API).

3.9.1.7 The CMS shall at a minimum support the following:

    3.9.1.7.1 Maintain the relationships between all service components and any related Incidents, problems, known errors, change and release documentation.

    3.9.1.7.2 Provide a customizable set of views for different stakeholders through the service lifecycle.

    3.9.1.7.3 Consolidate data from multiple physical CMDBs and data sources as necessary, which together constitute a federated CMS.

    3.9.1.7.4 Automate processes, discovery tools, inventory and validation tools, enterprise systems and network management tools, etc. to load and update the CMS.

    3.9.1.7.5 Map logical information to physical assets (e.g., business applications along with APM enriched information, software, DR RTO/RPO, billing attributes, virtual server instance associations with physical hosts).

    3.9.1.7.6 Support an extended, standardized data model for non-DIR Shared Technology Services assets enabling APM Customers to leverage the CMS as a single source of truth for Customer CIs.

Exhibit 2.1 Statement of Work   Page 63

3.9.1.8   Maintain the CMS to meet performance standards, to maximize efficiency, and to minimize outages, as necessary.

3.9.1.9   Designate performance standards for the CMS in the SMM, and approved by DIR.

3.9.1.10 Maintain, update, and implement the CMS archive processes and procedures needed to recover from an outage or corruption within designated timeframes in order to meet DIR and Customers' business requirements.

3.9.1.11 Provide CMS physical database management support, including providing backups and restores of data within designated timeframes.

3.9.1.12 Test and implement CMS database environment changes, as approved by DIR.

3.9.1.13 Proactively provide capacity planning for the CMS to prevent situations caused by lack of capacity (i.e., dataset or table space capacity events, full log files, etc.).

3.9.1.14 Correct situations caused by lack of CMS capacity within designated timeframes (i.e., dataset or table space capacity events, full log files, etc.).

3.9.2   Configuration Management Operations

The Successful Respondent shall, at a minimum:

3.9.2.1   Lead, develop and maintain a data model to standardize the definition of services, software, hardware, assets and relationships and maintain structures to support the proper documentation and maintenance of Configuration Items and Configuration Models.

    3.9.2.1.1   Design the data model to integrate with the APM data model to extend the CMS data model with APM-provided attribution.

    3.9.2.1.2   Lead and facilitate, amongst the APM services and DIR architecture teams, the definition of master product catalog (e.g., industry master product lists for software, hardware, cloud services) for use in validating APM CI's.

3.9.2.2   Verify that all CIs for the equipment, software, and applications are incorporated into the CMS.

3.9.2.3   For each CI, use at least the attributes specified by the Configuration Management policies and procedures defined in the SMM.

3.9.2.4   Ensure that there are adequate control mechanisms over CIs while maintaining a record of changes to CIs, versions, location and ownership so that CIs will not be added, modified, replaced or removed without appropriate controlling documentation and an appropriate procedure being followed.

3.9.2.5   Continually perform electronic logical validation of all equipment, software, applications and relationships used to provide the DIR Shared Technology Services in accordance with the Configuration Management Validation Plan, in order to:

Exhibit 2.1 Statement of Work   Page 64

3.9.2.5.1 Validate that any change to any Successful Respondent-managed CI attribute in the CMS is the result of an approved Service Request or Request For Change.

3.9.2.5.2 Verify the existence of CIs recorded in the CMS by providing logical validation of all CIs from the Service Component Provider(s) to the CMS and from CMS to the Service Component Provider(s).

3.9.2.5.3 Check the accuracy and completeness of the records and attributes in the CMS.

3.9.2.5.4 Reconcile APM provided master product lists (e.g., industry product lists for software, hardware, cloud services) to APM CI's identifying non-reference CI's.

3.9.2.5.5 Identify any CIs and attributes provided in DIR, Customer or Service Component Provider data sources that are not recorded in the CMS.

3.9.2.5.6 Identify any CIs and attributes in the CMS that are not provided by DIR, Customer or Service Component Provider data sources.

3.9.2.5.7 Formally record exceptions discovered from the validation effort.

3.9.2.5.8 Take corrective action through the Incident Management, Problem Management, or Request Management processes if electronic validation identifies any deficiency in the accuracy or completeness of the records in the CMS.

3.9.2.6 Provide snapshots of the current logical configuration of a service, system or set of configuration items upon request and for use in problem analysis, Incident restoration, security management, etc.

3.9.2.7 Verify configuration documentation before Changes are made to the live environment.

3.9.2.8 Maintain a secure audit trail of all CMS transactions.

3.9.3 Application Portfolio Management (APM) Systems and Processes

The goal of Application Portfolio Management is to describe the inventory of business applications and the resources (e.g., money, staff time, infrastructure) required to provide operational support of those applications over their lifetime. APM should guide the investment decisions for an application's lifecycle, particularly balancing between adding features, maintaining infrastructure currency, and modernizing the platform.

Application portfolio management is used to:

- Identify application investment requirements
- Identify and tracks costs
- Establish application lifecycle expectations
- Identify the lifecycles of the components supporting the business applications
- Measure, report, and adjust values and expectations
- Track against original expectations

Exhibit 2.1 Statement of Work   Page 65

- Track large changes to requirements over the life of the application

- Consolidate all the application aspects into a centralized repository

The Successful Respondent shall, at a minimum:

3.9.3.1   Provide and support an APM System that, at a minimum, provides:

3.9.3.1.1   An inventory of business applications and their relationships, dependencies, and key related components including the ability for the Customer to add, update and delete custom application attributes.

3.9.3.1.2   Integration of the APM System with the Successful Respondent provided CMS.

3.9.3.1.3   Integration of the APM service with CMDBs other than the Successful Respondent provided CMDB through standard published interfaces.

3.9.3.1.4   Definition of standards for storage of information on hardware instances, software installations, and relationship mapping.

3.9.3.1.5   Master product lists (e.g., industry product lists for software, hardware, cloud services) for use in identifying non-reference CIs, thereby enabling reference architecture governance.

3.9.3.1.6   Ability to support data quality management analysis on data quality based on integrated feeds for normalized third party software and hardware using standard, master product list taxonomy and defined data naming standards.

3.9.3.1.7   Ability to maintain and track application lifecycle information (e.g., release date, end of support, end of life) and classification information (e.g., build, run/maintain, migrate, retire).

3.9.3.1.8   Ability to maintain and track hardware and software components by: Hardware and software components with Original Equipment Manufacturer (OEM) support milestones (e.g., Release date, End-of- Support, End-of-Life).

3.9.3.1.9   Ability to maintain and track cost components of business applications (support, development, maintenance, hardware, software, project, etc.) and rollup those costs to a business application and to a portfolio based on allocation methods approved by DIR.

3.9.3.1.10 Identification of investment requirements for business applications including providing tracking and aggregated views for: estimation of costs to build, run, and maintain.

3.9.3.1.11 Ability to perform business analytics on APM services data.

3.9.3.2   Provide flexible data input methods that, at a minimum, include:

3.9.3.2.1   Provide a consistent, well-defined and user-friendly import process to add, update, map, reconcile and normalize data to ensure consistent refresh of the data components.

Exhibit 2.1 Statement of Work   Page 66

3.9.3.2.2 Provide intuitive online data input methods (e.g., online surveys) and related workflows to enable intuitive manual data submission, review and approval including input of CI's not supported by the DCS program.

3.9.3.2.3 Provide an automated import process to add, update, map reconcile and normalize data to ensure consistent refresh of the data components.

3.9.3.2.4 Support integration with Information Technology Financial Management (ITFM) systems to obtain and relate financial information to the APM applications.

3.9.3.2.5 Provide built-in project management or integration with third party project management products.

3.9.3.3 Provide visualizations and reporting at varying levels of detail that, at a minimum, include:

3.9.3.3.1 Measurement and reporting based on adjustable parameters and views.

3.9.3.3.2 Ability to generate reports via on demand and/or scheduled reporting

3.9.3.3.3 Ability to generate reports that show trends in data/information over time

3.9.3.3.4 Dashboards with modular views of multiple chart styles and roadmap layouts, drill down capability for any chart or roadmap to show detail, dynamic views by category of service, lifetime, priority, cost, value

3.9.3.3.5 Dynamically generated views at various levels of abstraction of relationships based on business area, business applications, hardware and software components, and funding.

3.9.3.3.6 Views that enable rationalization by DIR Customer, across DIR Customers, and the enterprise.

3.9.3.3.7 Roadmaps that provide visual presentation of relationships including: Business applications' relationships and dependencies, Common hardware and software components across all business applications, and a business application to its supporting hardware and software components.

3.9.3.3.8 Visual outputs that provide insight for prioritization and value propositions when evaluating business applications' current state, dependencies, and future solutions.

3.9.3.3.9 Multidimensional output views of all domains of Customer applications including views for: value quadrants, business application roadmaps, application comparisons relative to one another, prioritization comparisons based on value vs. cost, and technology dependencies, etc.

3.9.3.3.10 Ability to export data in a form that allows Customers to perform self-service external reporting.

3.9.3.3.11 Support data export and integration with external systems.

3.9.3.4 Provide multi-tenancy capabilities including:

3.9.3.4.1 Leverage of a common application structure across multiple Customers.

3.9.3.4.2 Data of all common tenant Customers can be rolled up for cross-Customer queries or merged reports.

Exhibit 2.1 Statement of Work   Page 67

      3.9.3.4.3   Maintenance of logical separation between Customer tenants supporting varying levels of access to data (e.g., access by role, group, Customer program area, Customer, or enterprise).

      3.9.3.4.4   Ability to expose shared business applications and appropriate level of related detail to DIR.

3.9.3.5   Implement the APM system including, at a minimum:

      3.9.3.5.1   Design the APM tool's configuration to meet the business requirements as approved by DIR.

      3.9.3.5.2   Configure and implement the APM system.

      3.9.3.5.3   Establish and verify data import, export, and reconciliation functions (automated and semi-automated) between the Successful Respondent's CMS.

      3.9.3.5.4   Provide the capabilities to support the integration with various types of other DIR Customer Configuration Items data repositories (e.g., standalone databases, Comma-separated Value (CSV) files).

      3.9.3.5.5   Leverage best practices supporting APM governance and integration APM solution in the form of: workflow, attribute classification and taxonomy definition, attribute data normalization, relationship mapping, and implementation of business application cost structures (examples of cost structures that support business applications are: application maintenance, development, and operations).

      3.9.3.5.6   Support Customer implementations into the APM capability including implementations involving Customers with different IT maturity levels.

      3.9.3.5.7   Coordinate activities between DIR, Customers, and the APM software vendor to create the technical backlog of user stories and to identify user testing and acceptance criteria for each enhancement.

      3.9.3.5.8   Establish APM Service governance model by engaging DIR and Customers to establish and implement governance policies and practices in the SMM which include, at a minimum:

            3.9.3.5.8.1 Description of available reports and dashboards.
            3.9.3.5.8.2 Data Model Diagram.
            3.9.3.5.8.3 Data Ingestion processes.
            3.9.3.5.8.4 Data Integration processes.
            3.9.3.5.8.5 APM Workflows.
            3.9.3.5.8.6 Data Input / Survey process.
            3.9.3.5.8.7 Multi-tenancy security model.
            3.9.3.5.8.8 Training materials for all users.

3.9.3.6   Maintain APM System to meet performance standards, to maximize efficiency, and to minimize outages, as necessary.

3.9.3.7   Designate performance standards for the APM System in the SMM, and approved by DIR.

3.9.3.8   Maintain, update, and implement the APM System archive processes and procedures

needed to recover from an outage or corruption within designated timeframes in order to meet DIR and Customers' business requirements.

3.9.3.9   Provide APM System physical database management support, including providing backups and restores of data within designated timeframes.

3.9.3.10 Test and implement APM database environment changes, as approved by DIR.

3.9.3.11 Proactively provide capacity planning for the APM System to prevent situations caused by lack of capacity (i.e., dataset or table space capacity events, full log files, etc.).

3.9.3.12 Correct situations caused by lack of APM System capacity within designated timeframes (i.e., dataset or table space capacity events, full log files, etc.).

3.9.4   Application Portfolio Management (APM) Operations

The Successful Respondent shall, at a minimum:

3.9.4.1   Provide services to introduce and onboard new DIR Customers to the APM service, including:

    3.9.4.1.1   Provide APM services solution as agreed to between the Parties.

3.9.4.2   Provide training to all APM users, including:

    3.9.4.2.1   Provide a range of initial and ongoing training to the various APM user types (e.g., DIR Customer APM administrators, DIR Customer business application stakeholders, technology stewards, financial stewards.).

3.9.4.3   Lead, develop and maintain a data model to standardize the definition of APM services and maintain structures to support the proper documentation and maintenance of APM Configuration Items.

    3.9.4.3.1   Design the data model to integrate with the CMS data model.

    3.9.4.3.2   Define the master product catalog (e.g. industry master product lists for software, hardware, cloud services) for use in validating APM CI's.

3.9.4.4   For each CI, use at least the attributes specified by the APM policies and procedures defined in the SMM.

3.9.4.5   Ensure that there are adequate control mechanisms over APM CIs enabling Customers to maintain APM information using self service features with automated change approvals and logging.

3.9.4.6   Continually perform electronic logical validation of all APM CIs and relationships used to provide the APM service in accordance with the APM Validation Plan, in order to:

    3.9.4.6.1   Validate that any change to any CI attribute in APM is the result of an approved APM update.

    3.9.4.6.2   Check the completeness of the records and attributes in APM.

Exhibit 2.1 Statement of Work   Page 69

3.9.4.6.3 Reconcile APM provided master product lists (e.g. industry product lists for software, hardware, cloud services) to APM CI's identifying non-reference CI's.

3.9.4.6.4 Take corrective action through the Incident Management, Problem Management, or Request Management processes if electronic validation identifies any deficiency in the accuracy or completeness of the records in APM.

3.9.4.7 Provide snapshots of the current logical configuration of a service, system or set of configuration items upon request and for use in problem analysis, Incident restoration, security management, etc.

3.9.4.8 Verify configuration documentation before Changes are made to the live environment.

3.9.4.9 Maintain a secure audit trail of all APM transactions.

3.10 IT Service Continuity Management

IT Service Continuity Management (ITSCM) supports the State's overall Business Continuity and Disaster Recovery (DR) process by ensuring the required IT technical and services operations (including computer systems, networks, Applications, data repositories, telecommunications, environment, technical support and Service Desk) can be recovered within required and agreed business timeframes. MSI must provide ITSCM as described in this **Exhibit 2.1 Multi-sourcing Services Integrator Statement of Work** and **Exhibit 2.3 IT Service Management Continuity**.

DIR retains the authority to declare a disaster at any location where DIR's Shared Services are performed. This includes:

1. DCS Consolidated Data Centers;

2. DIR Customer facilities;

3. Successful Respondent facilities; and

4. SCP facilities.

At a high-level, the Successful Respondent shall, at a minimum, provide personnel with infrastructure and application disaster recovery expertise to actively contribute to the integrity of disaster recovery strategy and planning processes, and disaster recovery project management expertise to effectively and efficiently lead testing and recovery activities.

SCPs will provide architecture and personnel with technical expertise to support their respective disaster recovery strategy and planning activities, and execute testing and recovery responsibilities.

Application owners (e.g., DIR Customers, MAS SCPs, Texas.Gov SCPs) are responsible for participating in planning and performing application-related testing and recovery responsibilities.

Exhibit 2.1 Statement of Work   Page 70

The effectiveness of IT Service Continuity Management will be measured by the Key SLAs (DR Test Report Delivery & DR Test Plan Objectives Met) defined in **Exhibit 3.1 Service Level Matrix** and **Exhibit 3.2 Service Level Definitions.**

3.10.1 IT Service Continuity Management Program Management

The Successful Respondent is responsible for establishing and maintaining the processes and framework required to manage the ITSCM program, including the creation and maintenance of program standards, processes, templates, tracking, and reporting.

The Successful Respondent shall, at a minimum:

3.10.1.1 Effectively implement and maintain DR processes and program operations, including:

> 3.10.1.1.1 Scope, methods, roles and activities for defining Disaster Recovery Plans (DRPs) and Technical Recovery Guides (TRGs) requirements.
>
> 3.10.1.1.2 Contents and use of DRPs and TRGs.
>
> 3.10.1.1.3 Methods, tools, roles and activities for engaging DIR Customers on ITSCM and conducting DR exercises.
>
> 3.10.1.1.4 Methods, tools, roles and activities for monitoring and reporting on ITSCM activity and activities for evolving metrics where ITSCM is not meeting Customer business goals.

3.10.1.2 Effectively execute the ITSCM processes, ensuring the SCPs are actively maintaining DRPs and TRGs that support DIR and Customer Business Continuity Plans (BCPs).

3.10.1.3 Lead and coordinate ongoing DRP operation and maintenance and regular testing.

> 3.10.1.3.1 Participate in regular Risk Analysis and Management exercises, particularly in conjunction with the business and the Availability Management and Security Management processes, that manage IT services within an agreed level of business risk.
>
> 3.10.1.3.2 Provide advice and guidance to other business and IT areas on DR related issues.
>
> 3.10.1.3.3 Ensure appropriate continuity and recovery mechanisms are in place to meet or exceed the agreed Customer targets.

3.10.1.4 Assess and report on the impact of DRPs and TRGs changes.

3.10.1.5 Verify the SCPs have the necessary Third Party Vendors contacts to support DRPs.

3.10.1.6 Communicate and coordinate the ITSCM process within MSI's own organization, SCPs, DIR, Customers, and designated Third Party Vendor(s); including:

> 3.10.1.6.1 Coordinate ITSCM activities across all functions that provide Customer Services.
>
> 3.10.1.6.2 Conduct regularly scheduled ITSCM meetings.
>
> 3.10.1.6.3 Document and publish ITSCM meetings status reports to relevant stakeholders.

Exhibit 2.1 Statement of Work   Page 71

3.10.1.7 Following any disaster, conduct a post-disaster meeting with SCPs, DIR, and DIR Customers to identify and understand the cause of the disaster; and develop plans to eliminate or mitigate future occurrences.

3.10.1.8 At all times, maintain strict compliance with the DR policies, standards, and procedures contained in DIR's and Customers' DRPs.

3.10.1.9 Train Successful Respondent, SCPs, DIR, DIR Customers, and designated Third Party Vendor personnel in DR procedures, and implement a process to obtain immediate access to DR procedures in a disaster situation.

3.10.1.10 Provide an effective program of on-going activities to support the DRPs, including at a minimum the following:

3.10.1.10.1 Conduct a regular review of ITSCM process to ensure they remain current.

3.10.1.10.2 Establish and maintain an on-going program of regular testing to ensure the critical components of the strategy are tested and align with business needs.

3.10.1.10.3 Establish and maintain an ongoing program to monitor and evaluate the backup and recovery of IT service to ensure they will operate when needed during a disaster.

3.10.1.10.4 Provide effective integration with the Change Management process to ensure changes are assessed for their potential impact on the ITSCM plans.

3.10.1.11 Ensure SCPs provide and maintain backups, file recovery capabilities, and historical data files and Software (including source code) utilized to process data.

3.10.1.12 Perform ITSCM functions in compliance with DR plan standards and procedures, and no less stringent than industry best practice standards and procedures.

3.10.2 Business Continuity

DIR and DIR Customers will retain responsibility for their Business Continuity plans and management activities.

3.10.3 Disaster Recovery Planning

3.10.3.1 The Successful Respondent shall coordinate the development, maintenance, testing, and, in the event of a disaster, DRP execution at the DIR Shared Technology Services level.

3.10.3.2 The Successful Respondent shall develop and modify the DIR Shared Technology Services DRP in coordination with DIR, DIR Customers, and SCPs. Such plans must comply with **Exhibit 2.3 IT Service Management Continuity** and the established DIR Shared Service Disaster Recovery Priority. DIR and DIR Customers will approve DRPs and modifications.

3.10.3.3 The Successful Respondent shall, at a minimum:

Exhibit 2.1 Statement of Work   Page 72

3.10.3.3.1 Effectively manage and maintain the DIR and DIR Customer DRPs, as they exist on the Effective Date.

3.10.3.3.2 Coordinate the creation of new DIR Customer and/or New Service Component DRPs as requested.

3.10.3.3.3 Maintain and continually program manage the enhancement of DIR's and DIR Customers' DRPs and TRGs throughout the Agreement Term, including enhancements required due to the introduction and use of new technologies (Equipment, Software, Applications, etc.), Resource Units, processes, business functions, locations, and priorities.

3.10.3.3.4 With DIR Customers' input, document DIR Customers' DR priorities based on DIR priorities.

3.10.3.3.5 Document the methods, processes and timeframes that allow DIR Customers to change priorities, as specified in SMM.

3.10.3.3.6 With DIR and DIR Customers' input and approval, develop a process that identifies and maintains the list of mission-critical Applications.

3.10.3.3.7 Recommend to DIR and DIR Customers security measures to incorporate, as defined for normal operations, into the DRPs.

3.10.3.3.8 Maintain a list of key personnel contacts and notification procedures for the Successful Respondent, SCPs, DIR, DIR Customers, and Third Party Vendors.

3.10.3.3.9 Comply with DIR's definition and procedures for declaring a disaster, as defined in the DIR-approved SMM.

3.10.3.3.10   Verify SCPs' Application and System Software backups support RTO and RPO objectives for each Customer Application.

3.10.4 Disaster Recovery Testing

For DIR Shared Technology Services, and in coordination with DIR, DIR Customers, and the SCPs, the Successful Respondent shall develop and modify DR test plans, including test scheduling and project management, and issue identification and logging resulting from the testing. DR tests will be scheduled in compliance with **Exhibit 2.3 IT Service Management Continuity**.

The Successful Respondent shall, at a minimum:

3.10.4.1 Establish joint test objectives with DIR and DIR Customers designed to verify Services will be available within established timeframe. Designate test objectives for which the SCP is accountable separate from the test objectives for which the DIR Customer is accountable.

3.10.4.2 Coordinate test plan acceptance with DIR, DIR Customers, and SCPs.

3.10.4.3 Schedule testing dates annually with DIR Customer's approval and give DIR and DIR Customers the opportunity to observe and participate. After annual planning, changes to the testing schedule will be considered based on business requirements, test environments, and availability of the Successful Respondent, SCP(s), and DIR Customer resources.

Exhibit 2.1 Statement of Work   Page 73

3.10.4.4 Test DRP components as required, coordinating the efforts of DIR, DIR Customers, and SCPs.

3.10.4.5 Record and report to DIR when a DIR Customer chooses not to test, including the identification of the affected DRPs and Applications.

3.10.4.6 Collect Authorized User feedback regarding the test and adequacy of continuity.

3.10.4.7 Provide DIR and Customers with a formal report of the test results within thirty (30) calendar days of each test. At a minimum, these reports must include:

    3.10.4.7.1 Results achieved and comparisons to the measures and goals identified in the respective test plans.

    3.10.4.7.2 Authorized User feedback as to the adequacy of continuity for their respective areas.

    3.10.4.7.3 Plan and schedule to remedy any gaps revealed during testing.

3.10.4.8 Coordinate responsibilities with DIR Customers and SCPs to ensure Application integrity exists after restoration in accordance with DRP.

3.10.4.9 Retest within ninety (90) days, without additional charge, if test fails to achieve specified results due to Successful Respondent's failure to perform its responsibilities.

3.10.4.10   Update the DRPs upon re-testing and verify the remedy was successful.

3.10.5 Disaster Recovery Activities

For DIR Shared Technology Services and in coordination with DIR, DIR Customers and the SCPs, the Successful Respondent shall be responsible for project managing activities required to recover DIR Shared Technology Services in the event a disaster is declared.

The Successful Respondent shall, at a minimum:

3.10.5.1 Report disasters (or potential disasters) to DIR and Customers immediately upon identification based on parameters defined in the DRPs, and consult with DIR for an official disaster declaration is appropriate.

3.10.5.2 Recommend to DIR when to declare a disaster and execute the disaster declaration in accordance with procedures existing at the time of declaration.

3.10.5.3 Lead DRP execution and coordinate required tasks with affected SCPs and DIR Customers including:

    3.10.5.3.1 Equipment installation or installation coordination.

    3.10.5.3.2 Equipment operation.

    3.10.5.3.3 Software restoration.

    3.10.5.3.4 Verification that data is recovered to the appropriate point in time.

    3.10.5.3.5 Coordinate and support DIR Customers as defined in the DRP to bring Applications into production ready mode.

Exhibit 2.1 Statement of Work   Page 74

3.10.5.3.6 In accordance with the DRPs, determine what resources to deploy in support of the recovery effort.

3.10.5.4 Conduct, supervise, and administer the operation and implementation of such resources.

3.10.5.5 Provide additional resources as necessary to support the disaster recovery coordination efforts.

3.10.5.6 In accordance with DRPs, develop a plan for the return of Services to the original processing site or an alternate(s) site specified and agreed to by DIR in the DRPs.

3.10.5.7 Provide for a return of readiness to respond to a disaster, as set forth in the DRPs.

3.10.6 Return to Normal Operations Activities

For DIR Shared Technology Services and in coordination with DIR, DIR Customers, and SCPs, the Successful Respondent shall be responsible for project managing activities required to return DIR Shared Technology Services to normal operations after a disaster.

The Successful Respondent shall, at a minimum:

3.10.6.1 Project manage the activities required to return DIR Customer services from the disaster recovery target to replacement infrastructure as normal operations.

3.10.6.2 Coordinate SCP, DIR, and DIR Customer responsibilities to solution and cost replacement infrastructure needs.

3.10.6.3 Report status, issues and risks in transitioning to replacement infrastructure.

3.10.7 Crisis Management

Crisis management may be necessary depending on the type of business or geographic location where Services are being performed (e.g., hurricanes, tornados, riots, terrorist threats).

The Successful Respondent shall, at a minimum:

3.10.7.1 Provide increased support when a crisis is declared.

3.10.7.2 Provide alternative communications methods (e.g., out of band communications support).

3.10.7.3 Follow statewide notification pyramid alert support as documented in the applicable business continuity plan.

3.10.7.4 Follow DIR notification processes for any crisis event occurring in or relating to a Successful Respondent Facility, DIR Facility, or other facilities managed by the Successful Respondent in connection with the Services.

3.10.7.5 Implement crisis procedures per the DIR-approved SMM.

3.10.7.6 Support and communicate with the State's Emergency Management Council direction

Exhibit 2.1 Statement of Work   Page 75

as defined in **Exhibit 2.3 IT Service Management Continuity.**

3.11   Project and Program Management

Project Management provides a common way to execute and manage projects with the goal of delivering projects from request through completion, meeting DIR Customer requirements in terms of timing, quality, and cost. The Successful Respondent shall manage projects related to the Successful Respondent's Services.

Program Management provides a way to achieve a defined business objective through logically grouped and related projects. Given the relationship of projects to programs, the Successful Respondent is required to deploy an integrated platform and processes to enable both project and program management. The SCPs are expected to use the Project and Program Management (PPM) system as the single source of record for managing projects and Programs.

The effectiveness of Project Management will be measured by Critical SLAs (New Service Offering Request Fulfillment, New Customer Onboarding, Service Catalog Management) and Key SLAs (Solution Proposal Delivery, Solution Implementation) defined in **Exhibit 3.1 Service Level Matrix** and **Exhibit 3.2 Service Level Definitions.** In addition, effectiveness will be measured through the implementation of the Technology and Security Plans, defined in **Exhibit 3.3, Critical Deliverables.** Key Performance Indicators defined in **Exhibit 3.4 Performance Analytics** will also demonstrate whether project management is effectively improving Shared Services. The availability of Project and Program Management systems will be measured by the Critical SLA "MSI Shared Services Systems Availability," defined in **Exhibit 3.1 Service Level Matrix** and **Exhibit 3.2 Service Level Definitions**

At a high-level, the Successful Respondent shall:

3.11.1.1 Administer and manage SCP Project Pool hours, including, but not limited to, establishing pool management and usage processes, adhering to said processes, providing pool usage reporting to DIR and Governance groups as needed.

3.11.1.2 Under the direction of DIR, lead SCPs as appropriate to achieve the outcomes of Programs. Programs may be long term, short term, and/or ad hoc. Expected Cross-Functional programs upon Commencement include:

   3.11.1.2.1 Currency & Refresh – includes hardware and software currency

   3.11.1.2.2 Customer Outreach – includes identifying potential customers and developing solutions and cost estimates, and onboarding.

   3.11.1.2.3 Continuous Improvement Initiatives - includes routine Performance Management service delivery improvement plans, and ongoing initiatives to improve service delivery or improve Key Performance Indicator trends.

   3.11.1.2.4 Service Portfolio Management – includes the design, development and implementation of new services within DIR's shared services.

3.11.2 Project and Program Management System

The Successful Respondent shall, at a minimum:

Exhibit 2.1 Statement of Work   Page 76

3.11.2.1 Provide and maintain a PPM system that will serve as the single source of information regarding all projects and programs for Successful Respondent and SCPs project and program management. PPM system should include an automated workflow and tracking system to facilitate implementation, status reporting, resource allocations, etc.

3.11.2.2 Grant DIR and Customers access to the PPM system and allow DIR to monitor and view projects and programs on an ongoing basis.

3.11.2.3 Provide access to the PPM system to other SCPs, DIR, and DIR Customers, including all appropriate and required licenses and/or interfaces.

3.11.2.4 Ensure that all Project Management and Program Management data resides in the PPM system.

3.11.2.5 Integrate the PPM system with other systems for Service Management, including Incident Management, Problem Management, Change Management, Release Management, Configuration Management, Financial Management, Service Level Management.

3.11.2.6 Provide sufficient access to the PPM system allowing all Authorized Users with appropriate credentials to access content in accordance with their granted access rights. Authorized Users may be staff from SCP, DIR, DIR Customers, and Third Party Vendors.

3.11.2.7 Provide Successful Respondent personnel, SCP personnel, DIR, DIR Customers and authorized Third Party Vendors with appropriate training in using the PPM system.

3.11.2.8 Enable electronic visibility to Project Management and Program Management activities across all functions and SCPs that provide services to DIR Customers. The PPM system shall, at a minimum, support the following:

  3.11.2.8.1 Maintain the approved Program Management and Project Management methodology as defined in the SMM.
  3.11.2.8.2 Provide automated workflow to allow for projects to progress from request through to completion.
  3.11.2.8.3 Deploy and support the platform enabling the documentation and electronic publishing of integrated Project Management and Program Management status reports to all relevant stakeholders, including DIR, Customers, other SCPs and authorized Third Party Vendors.
  3.11.2.8.4 Provide a customizable set of views for different stakeholders through the project and program lifecycle.
  3.11.2.8.5 Provide executive, program, and project-level dashboards and reporting to allow for full project and program transparency.
  3.11.2.8.6 Provide for time tracking setup, project and program manager time tracking, Customer approval and reporting capabilities for Successful Respondent and SCPs.

Exhibit 2.1 Statement of Work   Page 77

3.11.2.9 Maintain the PPM system to meet performance standards, to maximize efficiency, and to minimize outages, as necessary.

3.11.2.10 Designate performance standards for the PPM system in the SMM.

3.12 Release Management

The purpose of Release Management is to build, test and deliver specified Services that will accomplish the stakeholders' requirements and deliver the intended objectives.

The effectiveness of Release Management will be measured by the Key SLA Change Management Effectiveness defined in **Exhibit 3.1 Service Level Matrix** and **Exhibit 3.2 Service Level Definitions.** The availability of Release Management systems will be measured by the Critical SLA "MSI Shared Services Systems Availability," defined in **Exhibit 3.1 Service Level Matrix** and **Exhibit 3.2 Service Level Definitions**

3.12.1 Release Management Systems and Processes

The Successful Respondent shall, at a minimum:

3.12.1.1 Work with SCP(s) to develop and establish a Release and distribution process so that each Change to Services is controlled, tested, traceable, authorized, and implemented in a structured manner.

3.12.1.2 Define and establish Release Management systems and process which support the following:

3.12.1.2.1 Define roles and responsibilities for Service Component Providers and Customers to ensure the provision of requested support as needed for a successful deployment.

3.12.1.2.2 Define agreed upon release and deployment plans, including the overall Release Management Plan and Release schedule, with DIR and Customers.

3.12.1.2.3 Ensure that each release package consists of a set of related assets and service components that are compatible with each other.

3.12.1.2.4 Ensure that integrity of a release package and its constituent components is maintained throughout the transition activities and recorded accurately in the AIMS and CMS.

3.12.1.2.5 Provide capabilities for Service Component Providers to manage release testing for traditional waterfall and agile methodologies including tracking of use cases, stories, sprints, defects and other release and release testing concepts.

3.12.1.2.6 Ensure that release and deployment packages can be tracked, installed, tested, verified, and/or uninstalled or backed out if appropriate.

3.12.1.2.7 Ensure that organization and stakeholder change is managed during the release and deployment activities.

3.12.1.2.8 Provide capabilities to record and manage defects, deviations, risks, issues related to the new or changed service.

Exhibit 2.1 Statement of Work   Page 78

3.12.1.2.9 Ensure that there is knowledge transfer to enable the customers and users to optimize their use of the service to support their business activities.

3.12.1.2.10 Ensure that skills and knowledge are transferred to operations and support staff to enable them to effectively and efficiently deliver, support and maintain the service in compliance with required warranties and service levels.

3.12.1.2.11 Record the identification, design and management of releases and release packages.

3.12.1.2.12 Support the planning, execution and management of testing methods, tools and procedures.

3.12.1.2.13 Define release success / failure criteria for each point in the Release lifecycle.

3.12.1.2.14 Establish measurement processes to record the success and failure of Releases, including recording Incidents related to Release activities and in the period following a Release.

4 BUSINESS MANAGEMENT

4.1 Operational Intelligence

Operational Intelligence provides transparency into the overall operation and performance of all Services and provides the management information and reporting capabilities to support the data intelligence requirements. These requirements include the implementation and operation of Operational Reports, Operational Measures, Service Level Measures, Key Performance Indicators, Contract Performance Incentives and overall Performance Analytics, as defined in **Exhibit 3.0 Performance Model** and **Exhibit 4.0 Business Model**.

Operational Intelligence will be used highly by DIR leadership and DIR's Customer Relationship Management. The quality and effectiveness of the Operational Intelligence tools and services will be measured in the Key Performance Indicators defined in **Exhibit 3.4 Performance Analytics** and Customer Satisfaction Surveys defined in **Exhibit 3.5 Customer Satisfaction.** The availability of Operational Intelligence systems will be measured by the Critical SLA "MSI Shared Services Systems Availability," defined in **Exhibit 3.1 Service Level Matrix** and **Exhibit 3.2 Service Level Definitions**

4.1.1 Operational Intelligence System

The Successful Respondent shall, at a minimum:

4.1.1.1 Provide and maintain an Operational Intelligence Management System that will serve as the collector and reporting system for data provided by MSI and Service Component Providers.

4.1.1.2 The Operational Intelligence Management System shall at a minimum provide accurate, current data for Operational Reports, Operational Measures, Advanced Analytics, Key Performance Indicators, Contract Performance Incentives and integrate with the core MSI Shared Services Systems (e.g., Service Level Management System, IT Financial Management System).

Exhibit 2.1 Statement of Work   Page 79

4.1.2   Operational Intelligence Operations

The Successful Respondent shall, at a minimum:

4.1.2.1   Create automated information exchange between and among Successful Respondent, SCPs, DIR, DIR Customers, and/or CSPs to improve end-to-end Operational Intelligence.

4.1.2.2   Direct and manage Operational Intelligence activities across all functions and SCPs that provide services to DIR Customers.

4.1.2.3   Conduct regularly scheduled Operational Intelligence meetings, included those associated with the requirements for governance as described in **Exhibit 1.2 Governance**.

4.1.2.4   Document and publish Operational Intelligence meetings status reports to all relevant stakeholders.

4.1.2.5   Implement, operate, and manage the Operational Intelligence capability to support the Operational Intelligence framework (Operational Reports, Operating Measures, Key Performance Indicators, Contract Performance Incentives – collectively "Reports") as described in **Exhibit 3.0 Performance Model** and to support the following requirements:

  4.1.2.5.1   Requirements, Data Collection and Report Generation
  4.1.2.5.2   Work closely with SCPs and DIR to capture Report Requirements.
  4.1.2.5.3   Collect required data from all SCPs.
  4.1.2.5.4   Implement and maintain the system and business logic to derive the Reports.
  4.1.2.5.5   Generate and publish accurate, timely Reports on behalf of all Service Providers and to DIR and Customers.

4.1.3   Validation and Improvement

The Successful Respondent shall, at a minimum:

4.1.3.1   Regularly validate Report data and business logic to ensure accurate reporting.

4.1.3.2   Proactively monitor Operational Intelligence processes and data looking for opportunities to streamline activities and continuously strive to improve service performance.

4.1.3.3   Identify and analyze issues, anomalies or trends which indicate risk in achieving accurate Reports.

4.1.4   Issue Escalation and Resolution

The Successful Respondent shall, at a minimum:

4.1.4.1   Ensure SCPs provide accurate, timely information to Report requirement achievement.

Exhibit 2.1 Statement of Work   Page 80

4.1.4.2 Identify, log, and manage the resolution of Report issues across DIR, SCPs, the Successful Respondent, and DIR Customers.

4.1.4.3 Serve as an escalation point for DIR, DIR Customer, and SCP reporting issues.

4.1.5 Advanced Analytics

The Successful Respondent shall, at a minimum:

4.1.5.1 Provide an integrated, web-based application for reporting and analyzing operational and business service performance which is accessible by authorized DIR, DIR Customers, Successful Respondent, and SCPs.

4.1.5.2 Provide pre-defined dynamic and interactive reports and dashboards which enable the Authorized Users to easily analyze the data to glean insight and determine action to improve the quality of processes and services.

4.1.5.3 Create and maintain a Report guide that describes each Report along with the name, description, business logic and calculations, input data and calculation logic, data exclusions and other criteria.

4.1.5.4 Manage activities required for additions, deletions, and modifications to Reports.

4.1.5.5 Provide all Reports in an integrated web-based and mobile accessible system allowing access

4.1.5.6 Maintain consistent use of reporting standards, formats, and so forth across Successful Respondent and SCPs.

4.1.5.7 Create Operational Intelligence presentations for DIR to present to DIR's Board, STC Governance, and DIR's executive leadership on a routine basis.

4.2 Service Level Management

Service Level Management will maintain and gradually improve business-aligned IT service quality through a constant cycle of agreeing, monitoring, reporting, and reviewing IT service achievements and through instigating actions to eradicate unacceptable levels of service in compliance with the Severity Levels, as described in **Exhibit 3.0 Performance Model**.

The Successful Respondent's service level performance will be measured by the Critical and Key SLAs defined in **Exhibit 3.1 Service Level Matrix** and **Exhibit 3.2 Service Level Definitions,** measured through the Successful Respondent's SLA Management system and process. The Successful Respondent is also required to measure all SCP's service level attainment through the SLA Management system and process. The availability of Service Level Management systems will be measured by the Critical SLA "MSI Shared Services Systems Availability," defined in **Exhibit 3.1 Service Level Matrix** and **Exhibit 3.2 Service Level Definitions**

Exhibit 2.1 Statement of Work   Page 81

Successful Respondent shall create any Operating Level Agreements necessary with any or all SCPs to ensure Successful Respondent's performance to attain its own service levels, as defined in **Exhibit 3.6 Operating Agreements.**

4.2.1   Service Level Management System

The Successful Respondent shall, at a minimum:

4.2.1.1   Provide and maintain a Service Level Management System that will serve as the collector and reporting system for performance data provided by the Successful Respondent, SCPs and CSPs.

4.2.1.2   Integrate the Service Level Management System with other systems for Service Management (e.g., Incident Management, Problem Management, Operational Intelligence, Asset Inventory and Management, Configuration Management).

4.2.1.3   Provide specifications (data, format, type, frequency, etc.) and work with SCPs and CSPs to enable interfaces that support data exchange between SCP/CSP systems and the MSI service level management system.

4.2.1.4   Limit access to the Service Level Management System to the agreed users who require access to the system, as approved by DIR.

4.2.1.5   Provide Successful Respondent personnel and Authorized Users with appropriate training in using the Service Level Management System.

4.2.1.6   The Service Level Management System shall at a minimum support the following:

  4.2.1.6.1   Support the key Service Level Management processes (e.g., Data Collection, Validation, Reporting, Exceptions, Issue Resolution, and Improvement Plans); and

  4.2.1.6.2   Integration with the Operational Intelligence System.

4.2.2   Service Level Management Operations

The Successful Respondent shall, at a minimum:

4.2.2.1   Coordinate and operate Service Level Management activities across all functions, SCPs, CSPs, and DIR Customer Sites that provide services to DIR Customers.

4.2.2.2   Conduct regularly scheduled Service Level Management meetings, including those associated with the requirements for governance as described in **Exhibit 1.2 Governance**.

4.2.2.3   Document and publish Service Level Management meetings status reports to all relevant stakeholders.

4.2.2.4   Communicate and coordinate the Service Level Management processes and policies within Successful Respondent's own organization, SCPs, DIR, and DIR Customers.

Exhibit 2.1 Statement of Work   Page 82

4.2.2.5 Provide on-going methods for training Successful Respondent staff, SCPs, DIR, and DIR Customers on the Service Level Management Process.

4.2.2.6 Provide integrated compliance reporting for the monitoring and management of service levels contained in any agreement between DIR, SCPs and CSPs when the other SCP(s)/CSP(s) are contractually required to provide compliance reporting data in a mechanized format.

4.2.2.7 Report SLA attainment summarized by DIR Customer, SCP, CSP, Shared Service, and Enterprise in an automated, drill-down system.

4.2.2.8 Implement, operate and manage the Service Level Management capability to support the Service Level Management framework as described in **Exhibit 3.0 Performance Model** and to support the following requirements:

4.2.2.8.1 Communication

4.2.2.8.1.1 Act as a liaison to DIR, DIR Customers, CSPs and SCPs for Service Level reports and the management of Service Level performance.

4.2.2.8.1.2 Provide analysis and engaging education to ensure awareness and availability of information needed for effective performance management and measurement.

4.2.2.8.2 Data Collection

Collect required data from all SCPs, CSPs calculate SLA performance, and deliver accurate, timely SLA reports to DIR, SCP(s) and DIR Customers.

4.2.2.8.3 Performance Management

4.2.2.8.3.1 Regularly validate Service Level data and calculations to ensure compliance of Service Level measure reporting.

4.2.2.8.3.2 Proactively monitor Service Level processes and data looking for opportunities to streamline activities and manage programs that continuously strive to improve service performance.

4.2.2.8.3.3 Identify and analyze issues, anomalies or trends which indicate risk in achieving service level targets. Communicate analysis results to DIR and SCPs.

4.2.2.8.3.4 Use automated thresholds to manage Service Level target achievement, to ensure that situations where service targets are breached or threatened are rapidly identified and cost-effective actions implemented to reduce or avoid their potential impact.

4.2.2.8.4 Exceptions

4.2.2.8.4.1 Proactively monitor for Service Level exception requests from all SCPs and review each for accuracy and compliance to DIR-approved exception approval policy documented in the SMM and relevant SCP agreement with DIR.

4.2.2.8.4.2 Proactively identify CSP related Service Level exceptions and initiate service credit requests with the CSP.

Exhibit 2.1 Statement of Work   Page 83

4.2.2.8.4.3 Compile weekly list of exception requests across all SCPs/CSPs and submit to DIR for approval.

4.2.2.8.4.4 Post and process DIR's final exception decisions.

4.2.2.8.5 Issue Escalation and Resolution

4.2.2.8.5.1 Identify with SCPs/CSPs potential service level attainment risks and early missed performance to ensure service level achievement.

4.2.2.8.5.2 Identify, log, and manage the resolution of Service Level issues across DIR, SCPs, CSPs and DIR Customers. Resolve issues where possible. Escalate unresolved issues or disputes to DIR.

4.2.2.8.5.3 Serve as an escalation point for DIR, DIR Customers, and Successful Respondent service level reporting issues.

4.2.2.8.6 Review Meetings

4.2.2.8.6.1 Facilitate recurring SLA compliance review meetings which include DIR and SCP(s) and provide SLA support information.

4.2.2.8.6.2 Publish the final enterprise, shared service and Customer level SLA compliance reports after the results are approved for posting.

4.2.2.8.7 Service Level Improvement Plans

4.2.2.8.7.1 Conduct and manage the analysis, corrective actions, and service improvement initiatives directed specifically toward achievement of contractual Service Level Agreements of all SCPs/CSPs as well as the Successful Respondent.

4.2.2.8.7.2 Facilitate Service Level improvement kick-off and status meetings.

4.2.2.8.7.3 Manage the service improvement process through completion.

4.2.2.8.7.4 Track corrective and improvement actions.

4.2.2.8.7.5 Correlate implemented corrective and improvement actions to service performance results.

4.2.2.8.7.6 Assess the impact of tools, process or business changes on Service Levels and provide recommendations on proposed changes.

4.2.2.8.8 Credits and Earnback

Track Service Level Credits and Earnback (completed or lost) by SCP and the Successful Respondent, and provide updated Service Level Credit and Earnback Reports to DIR.

4.2.2.8.9 Reports

4.2.2.8.9.1 Generate and publish Service Level compliance reports on behalf of all SCPs/CSPs to DIR and DIR Customers.

4.2.2.9 Create and maintain a Service Level guide posted online for all stakeholders that describes each service level along with the name, description, calculation inclusions and exclusions, input data and calculation logic, data exclusions and other measurement criteria, as defined in **Exhibit 3.2 Service Level Definitions**.

4.2.2.10 Manage activities required for additions, deletions, and modifications to Service Levels.

4.2.2.11 Initiate and manage periodic Service Level compliance management assessments to evaluate the compliance, accuracy, timeliness, and quality of Service Level reports.

Exhibit 2.1 Statement of Work   Page 84

4.3   Availability Management

Availability Management will ensure that the level of service availability delivered in all Services is matched to or exceeds the current and future needs of the business, in a cost-effective manner. Availability Management provides a point of focus and management for all availability-related issues, relating to both services and technology, ensuring that availability targets are established, measured and achieved.

The Successful Respondent's effectiveness in managing Service availability will be measured and evaluated by the attainment of SCP and Successful Respondent service levels, as well as Customer satisfaction measured in the Monthly Customer Scorecard, defined in **Exhibit 3.5, Customer Satisfaction.** The availability of Availability Management systems will be measured by the Critical SLA "MSI Shared Services Systems Availability," defined in **Exhibit 3.1 Service Level Matrix** and **Exhibit 3.2 Service Level Definitions**

4.3.1   Availability Management System and Process

The Successful Respondent shall, at a minimum, develop an Availability Management process with Successful Respondent and other SCPs that will meet the following objectives:

4.3.1.1   Produce and maintain a Digital Availability Plan that reflects the current and future needs of DIR and Customers.

4.3.1.2   Identify proactive measures SCPs and Successful Respondent can implement that would avoid potential Service Availability issues.

4.3.1.3   Ensure that proactive measures to improve the availability of services are implemented wherever it is cost-justifiable to do so.

4.3.2   Availability Management Operations

The Successful Respondent shall, at a minimum:

4.3.2.1   Provide and manage an Availability Management operation that will provide the following activities:

4.3.2.1.1   Establish measures and reporting of availability, reliability, and maintainability that reflect DIR and DIR Customers and IT support organization perspectives.

4.3.2.1.2   Monitor, measure, analyze and report IT service and component availability.

4.3.2.1.3   Monitor and provide trend analysis of the availability, reliability, and maintainability of IT components.

4.3.2.1.4   Review IT service and component availability and identifying those that fail to meet availability and reliability targets.

4.3.2.1.5   Investigate the underlying reasons for failing to meet availability and reliability targets, report, and initiate remediation plans through defined processes (e.g., Incident Management, Problem Management, Request Management, Project Management, Program Management).

4.3.2.1.6   Provide early warning or advice to DIR, SCPs and Customers of potential or actual Availability or reliability issues.

Exhibit 2.1 Statement of Work   Page 85

4.3.2.2 Produce a Digital Availability Plan that is agreed by DIR and that incorporates the following, organized by DIR, DIR Customer, SCP, and Third Party:

   4.3.2.2.1 Actual levels of availability, mean time between failure, mean time to restore, and trends provided versus agreed levels of availability for IT services.

   4.3.2.2.2 As appropriate, include availability measurements that are business and customer-focused enabling near real-time business decisions.

   4.3.2.2.3 Include related actions being progressed through Incidents, Problems, Requests, Changes, Projects and Programs to address shortfalls or negative trends in availability for IT services.

   4.3.2.2.4 Provide the ability to drill-down from business services (e.g., applications), to IT services, to the lower-level resources and associated Incidents, Problems, Changes, Projects, and Requests.

   4.3.2.2.5 Retain at least twenty-four (24) months of Availability source data or in compliance with the DIR Customer Data Retention Schedule to enable trend analysis and to make such data available to DIR, DIR Customers, and SCPs.

   4.3.2.2.6 Provide the ability to initiate remediating actions on instances of unavailability through defined processes (e.g., Incident Management, Problem Management, Request Management, Project Management, Program Management)

4.4   IT Financial Management

Proper Financial Management provides cost-effective stewardship of DIR Shared Technology Services. The Successful Respondent shall provide Financial Management Services as described in the sections below and in **Exhibit 4 Business Model**.

The effectiveness of IT Financial Management will be measured by the accuracy of Customer invoices and volume of invoice disputes, the accuracy of financial forecasts, and the accuracy of data supplied to the Operational Intelligence systems. The effectiveness of invoice dispute resolution will be measured by the Critical SLA, Invoice Dispute Resolution defined in **Exhibit 3.1 Service Level Matrix** and **Exhibit 3.2 Service Level Definitions.**

The availability of IT Financial Management systems will be measured by the Critical SLA "MSI Shared Services Systems Availability," defined in **Exhibit 3.1 Service Level Matrix** and **Exhibit 3.2 Service Level Definitions.**

4.4.1   Enterprise Invoice Consolidation

The Successful Respondent shall, at a minimum:

4.4.1.1   Provide DIR with a monthly invoice that compiles Successful Respondent, SCP, and DIR Charges and reconciles with single monthly DIR Customer chargeback invoices.

4.4.1.2   Provide DIR with the supporting invoice detail necessary to facilitate DIR and DIR Customer payment to Successful Respondent and SCPs that are supplying Services under the Agreement.

4.4.1.3   Execute DIR-approved invoice validation process as approved in the SMM.

Exhibit 2.1 Statement of Work   Page 86

4.4.1.4   Report invoice validation results monthly, and identify anomalies based on DIR approved variance thresholds, prior to DIR Customer chargeback invoice release.

4.4.1.5   Provide DIR a monthly report confirming amounts paid to each SCP and any outstanding balance with sufficient detail for DIR to confirm the unpaid balances.

4.4.2   Chargeback and Utilization Tracking System

The Successful Respondent shall, at a minimum:

4.4.2.1   Provide and maintain a Chargeback and Utilization Tracking System (Chargeback System) that serves as the single billing tool and source for Successful Respondent, SCP, DIR, and DIR Customer financial information.

4.4.2.2   Provide Successful Respondent, SCP, DIR, and DIR Customer Chargeback System access based on DIR approved Authorized User profiles (e.g., by DIR Customer); including appropriate licensing and/or interfaces.

4.4.2.3   Integrate the Chargeback System with Successful Respondent and SCP Service Management Systems and tools, including, but not limited to Service Level Management, Capacity Management (CMIS), and Configuration Management (CMS/CMDB). Ensure the integration results in accurate and current billing data.

4.4.2.4   Enable Chargeback System integration with the SCPs' Financial Management Systems and designated Third Party Vendors as directed by DIR.

4.4.2.5   Provide DIR, DIR Customer, Successful Respondent, and SCPs Chargeback System training, including ongoing training for new Authorized Users.

4.4.2.6   Grant DIR access to Chargeback development, test and production systems.

4.4.2.7   Grant DIR access to Chargeback System detail source data and any database(s), and allow DIR to audit and validate on an ongoing basis.

4.4.2.8   Provide sufficient Chargeback System detail to support DIR and DIR Customers' State and Federal funding accounting, grant and audit requirements.

4.4.2.9   The Chargeback System shall, at a minimum, support the following:

4.4.2.9.1   Web-based DIR and DIR Customer access, transaction and Resource Unit drill down capability for all billing transactions, ad hoc query access, and soft copy billing downloads by Customer, account code and/or Resource Unit or Charge identifier(s) combination.

4.4.2.9.2   Accounting, usage tracking, self-service cost allocation, rate setting, invoice validation, DIR and DIR Customer reporting.

4.4.2.9.3   Collecting and aggregating monthly Resource Unit volumes and Charges, Requests for Service, and Service Level metric information from Successful Respondent and SCPs, including any DIR retained services.

Exhibit 2.1 Statement of Work   Page 87

      4.4.2.9.4 DIR and DIR Customer self-service access to input and maintain unique Account Code Identifiers and structures with effective dates, Resource Unit unique identifiers and cost category mapping at the lowest level of detail for Charges, Resource Units, New Services, One-Time Charges, and Pass-Through Expenses allowing for multiple lines of detail, multiple accounts and funding sources.

      4.4.2.9.5 Deploy Account Code Maintenance functionality to map resource unit volumes to DIR Customer Account Code Identifiers and integrate with Chargeback System.

      4.4.2.9.6 Electronic Chargeback detail as specified by DIR and DIR Customer.

      4.4.2.9.7 Electronic monthly billing detail and accounts receivables detail in DIR approved formats.

      4.4.2.9.8 DIR capability to access billing and volume information at summary and detail levels by DIR Customer and DIR Customer Account Code Identifiers.

      4.4.2.9.9 Customer capability to access billing and volume information for their Account Code Identifiers.

      4.4.2.9.10 Providing multiple SCP billing information to DIR and DIR Customers with Fixed and Variable Charges, Pass-Through Expenses, One-Time Charges, and miscellaneous Labor Charges implemented and maintained in common formats.

      4.4.2.9.11 Provide DIR and DIR Customer ability to load and maintain annual operating budget estimates and the ability to compare budgets with monthly invoiced Charges.

      4.4.2.9.12 Ability for system to accommodate monthly usage charges as well as time metered charges.

4.4.2.10 Maintain Chargeback System to DIR approved performance standards for maximizing efficiency and to minimize outages.

4.4.2.11 Provide Chargeback System logical configuration and database management support, including system backups and data restores within designated timeframes.

4.4.2.12 Develop, maintain, and implement DIR approved archive processes and procedures.

4.4.2.13 Develop and document Chargeback System performance and disaster recovery standards in the SMM.

4.4.2.14 Test and implement DIR approved Chargeback System changes via Change Management.

4.4.2.15 Proactively provide Chargeback System capacity planning and implement corrective measures to prevent system performance degradation or outages (i.e., dataset or table space capacity events, full log files, etc.).

4.4.2.16 Reports as described in **Exhibit 4.0 Business Model**, **Exhibit 4.3 Form of Invoice,** and **Exhibit 3.4 Performance Analytics** and ad hoc queries with appropriate local print

formatting.

4.4.2.17 Support Charges with detailed invoice reports and supporting utilization data at the SCP, DIR Customer, Resource Unit, Account Code Identifier level, as required.

4.4.3 Invoice Dispute Operations

The Successful Respondent shall, at a minimum:

4.4.3.1 Provide an invoice dispute resolution process and document in SMM.

4.4.3.2 Record, track and manage DIR and DIR Customer invoice disputes.

4.4.3.3 Research and review invoice disputes for completeness, supporting data accuracy and, when necessary, request clarifying data from DIR or DIR Customer.

4.4.3.4 Forward invoice disputes to the appropriate SCPs for processing within the agreed timeframes.

4.4.3.5 Facilitate invoice dispute resolution s with applicable SCPs, DIR, and DIR Customers within agreed timeframes as defined in the SMM.

4.4.3.6 Ensure invoice disputes Incidents are continually updated (at a minimum on a weekly basis) or as agreed to by DIR and defined in the SMM.

4.4.3.7 Provide DIR with invoice dispute metrics and dispute aging reports as agreed to by DIR and defined in the SMM.

4.4.3.8 Where applicable, calculate and assess Successful Respondent or SCP interest for disputes resulting in DIR and DIR Customer credits.

4.4.3.9 Allow DIR to monitor and validate invoice dispute process on an ongoing basis.

4.4.3.10 Provide a process for escalating disputes not resolved within the agreed timeframes established within DIR policies.

4.4.4 Forecasting Reporting

The Successful Respondent shall, at a minimum:

4.4.4.1 Leverage Chargeback, RFS, and Demand Management information to provide to DIR Financial planning and forecasting of planned resource consumption and Charges in accordance with **Exhibit 4.0 Business Model**.

4.4.4.2 Provide forecast reporting at the Customer, Resource Units, cost category (e.g., Programs, Divisions, Organization Units) and Resource Unit unique ID level, as required and documented in the SMM.

4.4.4.3 Integrate forecasting with Demand Management and Technology Planning processing.

Exhibit 2.1 Statement of Work   Page 89

4.4.5   DIR Consolidation Measurement Reporting and Optimization Program

Annually, the Successful Respondent shall perform a cost measurement process defined by DIR and produce a report that measures and evaluates the cost, cost savings and progress of DIR's Shared Services consolidation efforts.

The Successful Respondent shall, at a minimum:

4.4.5.1   Create, maintain, and implement a DIR Shared Technology Services Consolidation Measurement methodology approved by DIR and Governance and documented in the SMM.

4.4.5.2   On an annual basis, analyze DIR and Customer prior year's DIR Shared Technology Services consumption and Charges to document in a report if forecasted consolidation and financial objectives were achieved.

4.4.6   Intentionally Left Blank

4.4.7   Texas.gov Transaction Revenue Financial Management System and Reporting

The Successful Respondent shall, at a minimum:

4.4.7.1   Configure the Financial Management System to capture financial transaction data to include the Texas.gov transaction and payment details as reported by the Payment Processing SCP.

4.4.7.2   Provide Financial Management System functionality to allow for near real-time reporting of the transaction and payment details including reports as required to fully reconcile all attempted and failed transactions.

4.4.7.3   Provide Financial Management System functionality to allow DIR to develop self-generated reports on transactions and payment data by type of transaction, application, customer, etc.

4.4.7.4   Invoice DIR Customers for Texas.gov transaction fees.

4.4.7.5   Capture data with the appropriate level of detail in the Financial Management System so that all application and payment engine generated revenue is tied to each individual transaction. Additional reporting requirements are documented in **Attachment 3.4-A Reports**.

4.4.8   Billing Measurement Independent Verification and Validation

The Successful Respondent shall engage a Third-Party Vendor, approved by DIR, to independently verify and validate (IV&V) end to end MSI and SCP invoicing and Chargeback tools and processes, as well as source data and resulting Charges, to ensure such tools and processes are complete, accurate and producing consistent results.

The Successful Respondent shall, at a minimum:

4.4.8.1   Engage and manage a Third-Party Vendor to work with DIR to develop a billing

Exhibit 2.1 Statement of Work   Page 90

measurement risk assessment, and perform IV&V services on an ongoing basis as defined in **Exhibit 4.0**.

4.4.8.2   At DIR's direction, prioritize which Resource Units and Charges will be scheduled for review.

4.4.8.3   Collate, analyze and organize the IV&V results, and provide those results to DIR, MSI and Service Component Providers for corrective action.

4.4.8.4   Initiate Invoice Dispute as defined in the SMM, if appropriate.

4.4.8.5   Implement Successful Respondent-owned corrective actions. Monitor SCP corrective actions to ensure timely, accurate completion.

4.5   Customer Relationship Management

The Customer Relationship Management capability facilitates a connection with DIR Customers through a full understanding of their strategic and tactical business and information technology objectives, and managing the DIR Customers' DIR Shared Service demand, consumption and performance. The objective is to provide DIR Customers with a high degree of service transparency to make DIR Shared Technology Services a meaningful component within DIR Customers overall IT operation.

Given the critical importance of this capability, the Successful Respondent will assume the primary relationship role with DIR Customers, supported by the 2nd level escalation role of the DIR Enterprise Relationship Managers (ERMs). In this primary role, the Successful Respondent, will take leadership in providing the policies and overall Customer Relationship Management direction along with processes documentation, dashboard configuration and support, program performance reporting, customer satisfaction information and other related initiatives.

The Successful Respondent assigned to perform Customer Account Management, Customer Performance Analytics, Satisfaction Surveys, Customer Operations Management, Customer Project Management, and Customer Demand Management shall possess the training, education, experience, competence, and skill to perform such work.

The availability of Customer Relationship Management systems will be measured by the Critical SLA "MSI Shared Services Systems Availability," defined in **Exhibit 3.1 Service Level Matrix** and **Exhibit 3.2 Service Level Definitions.** The effectiveness of the Customer Relationship Management systems and information will be measured by the Monthly Customer Scorecard and Annual Customer Satisfaction survey, as defined in **Exhibit 3.5, Customer Satisfaction.** The effectiveness will also be measured by Key Performance Indicators defined in **Exhibit 3.4, Performance Analytics.**

4.5.1   Customer Relationship Management Systems and Processes

The Successful Respondent shall, at a minimum:

4.5.1.1   Develop and deploy Customer Relationship Management (CRM) systems that accesses and summarizes information from other MSI-provided tools and systems.

Exhibit 2.1 Statement of Work   Page 91

4.5.1.2   Under the direction of DIR, define the DIR Shared Technology Services CRM methodology and processes and implement the process into the Successful Respondent-provided CRM systems.

4.5.1.3   Integrate the CRM system with all Successful Respondent Shared Services Systems as needed to provide an efficient and effective platform to support the CRM function.

4.5.1.4   Limit access to the CRM systems to the agreed users who require access to the system, as approved by DIR.

4.5.1.5   Limit information presented in the CRM systems to the agreed roles who require access to the information, as approved by DIR.

4.5.2   Customer Account Management

Successful Respondent will staff and support the Customer Account Management function. This function will follow established processes and provide the primary interface to DIR Customers for required aspects of DIR Shared Technology Services from operations, projects, to demand planning. Additionally, the Successful Respondent will reinforce delivery execution through the Successful Respondent's cross-functional platform, reports and dashboards, and delivery escalation to the SCPs and DIR ERMs as defined in the SMM.

The Successful Respondent shall, at a minimum:

4.5.2.1   Serve as the primary DIR Customer contact for all DIR Shared Technology Services.

4.5.2.2   Have a firm understanding of the DIR Customer's business and IT objectives and requirements, customer portfolio of DIR Shared Technology Services, , and future technology direction and demand.

4.5.2.3   Develop and maintain effective DIR Customer relationships with the Business and IT key contacts, including the customer leadership team to include the DIR Customer CIO.

4.5.2.4   Coordinate and lead weekly, monthly, and/or quarterly customer meetings as defined in the SMM.

4.5.2.5   Work directly with DIR Customers to ensure a positive experience and results from DIR provided services.

4.5.2.6   Provide DIR Shared Technology Services communication to the DIR Customer as required.

4.5.2.7   Establishes and administers metrics and instruments to capture and benchmark customer satisfaction.

4.5.2.8   Act as point of contact, DIR Customer advocate, and liaison between representatives from DIR Customers and the Service Provider(s) regarding customer service issues, management issues, and escalated performance issues.

Exhibit 2.1 Statement of Work   Page 92

4.5.2.9 Responsible for DIR Shared Technology Services program customer satisfaction by tracking and managing all Customer service issues and collaborating with Service Providers for the development and management of customer service improvement plans.

4.5.2.10 Coordinate with DIR Customers, Service Provider(s), and DIR expert staff regarding root cause problem analysis/resolution and change management.

4.5.2.11 Enhance DIR Customer experience by performing root-cause analysis of DIR Customer impacting issues to identify improvement opportunities, recommend solutions, and implement process improvements.

4.5.2.12 Consistently evaluate processes and systems and champions the implementation of process improvement measures to generate higher efficiency.

4.5.2.13 Participate in Service Provider(s) status and problem solving meetings representing DIR Shared Technology Services and DIR Customer perspective; collaborates with other DIR technical experts to identify and analyze problems, trends, and issues and addresses them to resolution.

4.5.2.14 Assists with development and evaluation of customer service performance metrics in coordination with the DIR Governance and Performance Management specialist to facilitate evaluation of DIR performance in serving its customers.

4.5.3   Customer Performance Analytics

The Successful Respondent shall, at a minimum:

4.5.3.1   Leverage the Operational Intelligence capabilities to provide advanced customer analytics and operational insight thereby enabling data-driven customer intelligence.

4.5.3.2   Leverage DIR Customer Risks, Actions, Issues, Decisions (RAID) information to provide customer insight and coordinated transparency across DIR, MSI, SCP, and DIR Customers.

4.5.3.3   Leverage Service Level Performance compliance information to organize intuitive dashboards for the CRM team and DIR Customers to have clear visibility into service performance.

4.5.3.4   Leverage Chargeback and Forecasting reports and organize into intuitive dashboards for the CRM team and DIR Customers to have clear visibility into service financials (e.g., actuals, forecasts, disputes).

4.5.3.5   Leverage Incidents, Service Requests, Project, and Program reports and organize into intuitive work pipeline dashboards for the CRM team and DIR Customers to have clear visibility into all initiatives SCPs are performing for DIR Customers.

Exhibit 2.1 Statement of Work   Page 93

4.5.3.6   Compile the above information into electronic dashboard stories to facilitate periodic business reviews as defined in the SMM.

4.5.4   Satisfaction Surveys

The Successful Respondent shall, at a minimum:

4.5.4.1   For the annual Overall Customer Satisfaction Survey, the Successful Respondent shall, at a minimum:

   4.5.4.1.1   As specified in **Exhibit 3.5 Customer Satisfaction**, engage an independent Third Party Vendor, approved by DIR, to conduct "Overall Customer Satisfaction Surveys."

   4.5.4.1.2   Evaluate the survey results and, with DIR's approval, determine and implement appropriate action plans.

   4.5.4.1.3   Assist in customer survey outreach to increase participation rates.

   4.5.4.1.4   Performs follow up survey interviews with DIR Customers as needed.

4.5.4.2   For the monthly Customer Scorecard Survey, the Successful Respondent shall, at a minimum:

   4.5.4.2.1   Deploy a monthly Customer Scorecard Survey platform.

   4.5.4.2.2   Manage and administer the process to survey existing DIR Customers monthly and collect satisfaction scores across DIR Shared Technology Services.

   4.5.4.2.3   Collate, analyze, and organize the survey results, and provide those results to each SCP and DIR.

   4.5.4.2.4   Facilitate joint recurring meetings with DIR and SCP(s) to communicate and action the results.

   4.5.4.2.5   Provide an online tool to collect issues and action items identified in the Scorecard results, assigning each item to the appropriate SCP or the Successful Respondent to resolve.

   4.5.4.2.6   Provide process for SCPs to address Scorecard results.

   4.5.4.2.7   Perform DIR Customer outreach to increase participation rates prior to monthly submission schedules.

4.5.4.3   Project management and track the survey actions providing periodic progress and issues readouts.

4.5.5   Customer Operations Management

Successful Respondent will provide a liaison role between the DIR Customer and DIR Shared Technology Services to ensure the day to day operations are performing as intended. As an example, Customer Operations Management includes oversight of operational activities across all DIR Shared Technology Services, such as monitoring and event management, incident, request, change, asset, problem, security, backup and recovery, and IT service continuity management. The Successful Respondent shall, at a minimum:

4.5.5.1   Serve as the DIR Shared Technology Services representative for steady-state, day to

Exhibit 2.1 Statement of Work   Page 94

day operations across all DIR Shared Technology Services.

4.5.5.2 Establish, schedule and conduct DIR Shared Technology Services operations review meetings with the DIR Customer in accordance with the SMM.

4.5.5.3 Analyze and understand the DIR Customer technical and business operations environment and future direction and contribute towards the development of the DIR Customer's Technology Plan.

4.5.5.4 Be the primary escalation point of contact for all DIR Shared Technology Services operations, to include understanding and translating complex and technical information, driving issues to resolution, and communicating resolution outcomes to customers.

4.5.5.5 As required to address gaps or service issues, schedule and facilitate ad hoc meetings between the DIR Customer and SCP service delivery teams.

4.5.6 Customer Project Management

Successful Respondent will provide a liaison role between the DIR Customer and DIR Shared Technology Services to ensure projects (e.g., RFS, consolidation, etc.) are performing as intended. As an example, Customer Project Management includes oversight of projects related to RFS, consolidation, refresh, SCP-driven enterprise projects, various DIR programs, etc. The Successful Respondent shall, at a minimum:

4.5.6.1 Oversee the portfolio of projects for each DIR Customer and serve as the DIR Shared Technology Services representative for DIR Customer impacting programs and projects while leveraging the TSS and SCP project delivery resources to perform project management responsibilities.

4.5.6.2 Ensure alignment for the DIR Customer's portfolio of projects (e.g., scope, need by dates, delivery dates, resource availability, alignment with DIR Share Services overall program goals, etc.).

4.5.6.3 Establish, schedule and conduct DIR Shared Technology Services program and project review meetings with the DIR Customer in accordance with the SMM.

4.5.6.4 Analyze and understand DIR Customer projects and future demand and contribute towards the development of the DIR Customer's Technology Plan.

4.5.6.5 Ensure new technology and service deployments are properly coordinated and implemented per the processes defined in the SMM.

4.5.6.6 Be the primary escalation point of contact for all DIR Shared Technology Services programs and projects.

4.5.6.7 As required to address gaps or escalated program and project issues, schedule and facilitate ad hoc meetings between the DIR Customer and TSS or SCP project delivery teams.

Exhibit 2.1 Statement of Work   Page 95

4.5.7 Customer Demand Management

The Successful Respondent shall, at a minimum:

4.5.7.1 Lead demand management activities, as defined in the SMM, to capture future operations demand, project demand, and technology demands from DIR Customers to encourage DIR Customers to make the most effective use of all DIR Shared Technology Services resources, assist DIR to minimize its costs while maximizing the value DIR Customer's receive, and allow DIR to plan for and roll-out meaningful services.

4.5.7.2 Analyze Customer Configuration Item (CI) resources identifying optimization opportunities and presenting to the DIR Customer for action through Service Requests, Projects, and Programs (e.g., Facilitate CI Optimization for services Refresh opportunities, Facilitate CI Optimization for capacity overage situations, etc.).

4.5.7.3 Present New Services available in DIR Shared Technology Services to DIR Customers, to include providing a New Service overview, value proposition, and applicability analysis. Involve SCPs in presenting New Services opportunities when appropriate.

4.5.7.4 Provide DIR and DIR Customers with a report of the forecast of the demand queue by DIR Customer, projected resource requirements and resource constraints monthly.

4.5.7.5 Coordinate and facilitate DIR Customer discussions on their current consumption, provisioned capacity, and forecasted demand while capturing and actioning mitigating actions through Service Requests, Projects, and Programs.

4.5.7.6 Provide technology demand information into the Technology Planning and Financial Forecasting processes.

4.6 Service Delivery Management

The Successful Respondent shall provide delivery oversight of the SCPs operations not only to ensure the services are performing, but to also ensure the Successful Respondent is properly supporting and enabling the SCP operations.

The effectiveness of the Successful Respondent's Service Delivery Management will be measured by the extent to which all Shared Services SCPs meet or exceed service levels, the volume of Customer complaints, and the level of Customer satisfaction identified in Monthly Customer Scorecards.

The Successful Respondent shall, at a minimum:

4.6.1.1 Manage and coordinate the delivery activities of all SCPs providing services in support of DIR Shared Technology Services (e.g., DCS SCPs, Texas.gov SCPs, MAS SCPs, MSS SCPs, etc.).

4.6.1.2 Provide technical support liaisons with SCPs to resolve Incidents, Problems, and escalations with the DIR Shared Technology Services.

Exhibit 2.1 Statement of Work   Page 96

4.6.1.3   Monitor SCPs service delivery and performance of Services, including:

    4.6.1.3.1   Monitor compliance with any service levels contained in any agreement between DIR.

    4.6.1.3.2   Monitor Operating Measures and Operating Level Agreement attainment.

    4.6.1.3.3   Monitor performance for all DIR Shared Technology Services Enterprise capabilities (e.g., Incident Management, Request Management, Problem Management, Change Management).

4.6.1.4   Participate on periodic (e.g., daily, weekly) delivery operations calls or in other operations processes to ensure identified issues are being resolved timely and appropriately.

4.6.1.5   Evaluate customer satisfaction and scorecard feedback for issues and coordinate remediation through major processes and SCPs delivery meetings.

4.6.1.6   Notify DIR and the respective SCP(s) of the SCP(s) failure to perform in accordance with the provisions of its agreement.

4.6.1.7   Evaluate and recommend retention, modification, or termination of SCPs based on the performance or cost benefits to DIR as tracked by Successful Respondent.

4.6.1.8   In the event DIR procures cloud services directly from a public cloud provider, provide the capabilities to support the above requirements while managing public cloud services as a SCPs.

4.7   Capacity Management

Capacity Management assesses the current operations and future demands, pre-empting performance issues by taking the necessary actions before they occur.

The effectiveness of Capacity Management will be measured by the incident trends reported and the Service Quality Key Performance Indicator defined in **Exhibit 3.4, Performance Analytics.**

4.7.1   Capacity Management Information System (CMIS)

The Successful Respondent shall, at a minimum:

4.7.1.1   Implement, operate and manage a CMIS that will serve as the single source of Capacity information across all Services.

4.7.1.2   Implement a CMIS to aggregate Capacity Management information, provided by the SCPs, for all DIR Shared Technology Services.

4.7.1.3   Provide the means to automatically aggregate resource and system performance, system utilization, and capacity limits into the CMIS.

4.7.1.4   Provide the means to automatically calculate and forecast capacity requirements through trending of collected data anticipating capacity needs.

Exhibit 2.1 Statement of Work   Page 97

4.7.1.5   Provide the ability to action and track agreed capacity mitigations through associated Incidents, service requests, changes or projects.

4.7.1.6   The CMIS shall, at a minimum, collect and contain data and information for:

    4.7.1.6.1   Service data (e.g., transaction response times or batch job execution times).

    4.7.1.6.2   Technical capacity data (e.g., the maximum level of CPU utilization or the physical capacity of a particular hard disk).

    4.7.1.6.3   Technical utilization data (e.g., CPU utilization, paging rates, or bandwidth utilization).

    4.7.1.6.4   Service performance information.

    4.7.1.6.5   Information regarding thresholds, events and alerts.

    4.7.1.6.6   Related capacity mitigations through Incidents, requests, changes or projects.

    4.7.1.6.7   Identifying items by DIR Customer, DIR Shared Technology Services, SCP, Application, software, or hardware classification.

4.7.2   Capacity Management Operations

The Successful Respondent shall, at a minimum:

4.7.2.1   In an automated manner, aggregate capacity information including current capacity and utilization, trends, issues and actions at the DIR Customer, DIR Shared Technology Services, and SCP level.

4.7.2.2   Establish on-going Capacity Planning activities with DIR in coordination with other SCPs.

4.7.2.3   Initiate Incident Management, Problem Management, or Request Management activities as needed to address Capacity Management issues and trends.

4.7.2.4   Create, maintain and effectively execute a digital Capacity Plan that is agreed to by DIR.

4.7.2.5   Conduct regularly scheduled Capacity Management meetings.

4.7.2.6   Implement on-going activities with DIR and DIR Customers for Capacity Planning based on the Digital Capacity Plan. Communicate and schedule capacity management activities with other SCPs and designated Third Party Vendors.

4.7.2.7   Lead, conduct, and coordinate with DIR and SCPs at least quarterly on Capacity Planning.

4.7.2.8   Document and publish Capacity Management meetings status reports to all relevant stakeholders, including DIR, DIR Customers, other SCPs and authorized Third Party Vendors.

4.7.2.9   Collect and establish with DIR and DIR Customers appropriate thresholds for supporting the demand monitoring.

Exhibit 2.1 Statement of Work   Page 98

4.7.2.10 Incorporate appropriate capacity modeling to extrapolate forecasts of DIR Shared Technology Services growth and other changes in response to the projected DIR and Customer business and operational needs.

4.7.2.11 Coordinate and provide meaningful Capacity Planning input to the Technology Plan in support of requirements for long-range planning.

4.7.2.12 Coordinate and provide meaningful Capacity Planning input to the Refresh Plan in support of Refresh and Technical Currency.

4.7.2.13 Collect and establish with DIR and SCPs appropriate thresholds for capacity monitoring.

4.7.3 Digital Capacity Plan

The Digital Capacity Plan (Capacity Plan) will report on the current levels of resource utilization, Service performance, forecasted demand, captured DIR Customer demand and agreed mitigating actions.

The Successful Respondent shall, at a minimum:

4.7.3.1 Produce the Capacity Plan on monthly schedule.

4.7.3.2 Based on trended history, forecast demand out by twelve (12) months.

4.7.3.3 The Capacity Plan will at a minimum include the following:

> 4.7.3.3.1 The current Services, technology, and resources along with their respective current levels of capacity and utilization.
>
> 4.7.3.3.2 Active and historical Capacity Management-related Incidents, Problems, Requests, and Projects.
>
> 4.7.3.3.3 Historical Service Levels achieved.
>
> 4.7.3.3.4 Historical Changes.
>
> 4.7.3.3.5 Open and closed capacity related actions.
>
> 4.7.3.3.6 Electronically forecasted demand.
>
> 4.7.3.3.7 Forecasted demand provided by DIR Customer, DIR, or SCPs.

4.8   Risk Management Program

The Successful Respondent is charged with providing Risk Management related to the IT environment and services within the context of the DIR Shared Technology Services overall business risks. The goal of Risk Management includes the responsibility to quantify the impact to the business that a loss of service or asset would have, to determine the likelihood of a threat or vulnerability occurrence, and manage activity against the identified risks.

The Successful Respondent shall, at a minimum:

4.8.1.1 In support of DIR and DIR Shared Technology Services business risk management, develop and leverage the Risk Management process to program manage on-going Risk

Exhibit 2.1 Statement of Work   Page 99

Management activities for the identification, analysis, quantification, management and reduction of risks in the DIR Shared Technology Services environment.

4.8.1.2   Establish and facilitate on-going Risk Management and assessment activities with DIR and Service Component Providers.

4.8.1.3   To deliver a successful Risk Management Program, the MSI Risk Management program manager is responsible for executing the following:

   4.8.1.3.1   Analyze and document information related to threats, vulnerabilities, and risks.

   4.8.1.3.2   Host and facilitate annual risk summit with DIR and SCPs to perform a comprehensive review of risks, treatment plans and identify further remediating actions.

   4.8.1.3.3   Develop, maintain, and provide ongoing oversight of the Risk Management portfolio of prevention and treatment plans, initiatives and risk reduction projects.

   4.8.1.3.4   On a periodic basis as agreed to by DIR, program manage new and existing risk prevention and treatment plans and initiatives and monitor execution.

   4.8.1.3.5   On a periodic basis as agreed to by DIR, project manage and report on progress in executing risk reduction projects

   4.8.1.3.6   Track and generate Risk Management Program reporting on a monthly basis including prevention and treatment plan actions with status, and risk reduction measures as required by DIR.

   4.8.1.3.7   Under DIR's direction, improve the Risk Management process as required.

4.8.1.4   As required and in addition to the MSI Risk program manager, MSI Security representatives shall participate in the annual facilitated risk session and are responsible for the following:

   4.8.1.4.1   Facilitate and actively participate in sessions for threat, vulnerability, and risk identification.

   4.8.1.4.2   Consult with Successful Respondent teams and providing insight on threats and vulnerabilities relevant to Successful Respondent's scope of work.

   4.8.1.4.3   Identify and provide feedback on potential mitigation and management approaches.

   4.8.1.4.4   Facilitate the assignment of risk owners for identified items.

   4.8.1.4.5   Contribute to the review and approval of the Risk Management description, strategy, plan and initiatives.

4.8.1.5   As required for assigned risks, develop and execute the management plan and initiatives for assigned enterprise-level risks, providing the following:

   4.8.1.5.1   Ensure that the prioritized list of actions from the annual facilitated risk session is translated into a Risk Management plan, as defined in the SMM, with associated initiatives.

   4.8.1.5.2   Facilitate approval of the plan and initiative by applicable approvers.

Exhibit 2.1 Statement of Work   Page 100

    4.8.1.5.3 Execute the plan and initiatives and on a regular basis, provide updates to progress via the approved project management tool as defined in the SMM.

    4.8.1.5.4 Facilitate communications to stakeholders impacted by assigned risk management initiatives.

4.8.1.6 Provide Risk Management input to other programs toward the long-term reduction of risk in the environment (e.g., Capacity Plan, Technology Plan, Refresh Plan, etc.).

4.8.1.7 Support the Risk Management planning activities of DIR and DIR Customers in regards to the Services and IT environment.

4.9   Service Portfolio Management

From time to time, DIR is required and intends to, add or divest programs (or parts of programs), add, merge or split DIR Customers, change its organizations or reorganize its business units and add New Services and SCPs into the DIR portfolio. The Successful Respondent will perform certain functions at the request of DIR or DIR Customers to support such activities. The Successful Respondent will facilitate the addition of new DIR Customers and New Services by performing the ITIL functions of Service Strategy, Service Design and Service Transition.

The Successful Respondent shall, at a minimum:

4.9.1.1   Conform to the requirements and provide the Services associated with business additions, including the addition or divestment of new service components and/or new service component providers, mergers and other reorganizations as described in the MSA.

4.9.1.2   Assist DIR in planning, preparing and implementing any transition or changes related to the Services as a result of changes in the Service Portfolio (e.g., addition or removal of DIR Customers, DIR Shared Technology Services, SCPs).

4.9.1.3   Where DIR has an existing commitment to provide IT-related services to a business reorganization, divestiture, acquisition, consolidation, or relocation, provide the required Services on behalf of DIR.

4.9.1.4   Develop and document in the Service Management Manual processes and procedures to support changes in the Service Portfolio.

4.9.1.5   Project manage all stakeholders, including DIR, SCPs, and DIR Customers, to ensure the successful implementation of changes in the Service Portfolio.

4.9.1.6   Perform all required changes associated with changes in the Service Portfolio.

4.9.1.7   Perform all MSI Shared Services System infrastructure changes as required.

4.9.1.8   As New Services are implemented into the portfolio, adhere to all requirements as appropriate for the Service (e.g., security, disaster recovery, etc.).

4.9.1.9   Update the Service Portfolio with new projects or priorities in compliance with Project Management processes.

4.9.1.10   Execute all Service Portfolio change activities (e.g., onboarding additional DIR Customers into Successful Respondent Services or onboarding new DIR services or SCPs, removing DIR Customers or DIR Services, etc.).

4.9.1.11   Create and maintain service descriptions on public facing and DIR Customer facing portals for all DIR Shared Technology Services.

4.9.1.12   Describe and document all service portfolios for both current and potentially new DIR Customers.

Exhibit 2.1 Statement of Work   Page 102

4.9.1.13 Collect technical information and drive quality from SCPs and edit for clarity and readability.

4.9.1.14 Develop and maintain process to keep service descriptions current and accurate.

4.9.2   Addition and Removal of Customers

The Successful Respondent shall, at a minimum:

4.9.2.1   At the direction of DIR, develop and document in the Service Management Manual processes and procedures to support an efficient New DIR Customer outreach, solutioning, and onboarding process.

4.9.2.2   Perform a program management role to facilitate the addition or removal of DIR Customers, including:

4.9.2.2.1   Describe DIR services to potential DIR Customers.

4.9.2.2.2   Develop the plan, solution and transition in to operation for new DIR Customers.

4.9.2.2.3   Define related responsibilities for the SCPs and DIR Customers, and communicate responsibilities, tasks, and schedule to each party.

4.9.2.2.4   Project manage the activities related to the planning, solution development, and transition out of operation for exiting DIR Customers.

4.9.2.2.5   Engage in activities relative to planning and developing solutions for proposals to transition and support potential DIR Customers.

4.9.2.2.6   Add or remove users, organizations, and DIR Customers to Successful Respondent processes and Successful Respondent Shared Services Systems (e.g., Collaboration Portal, Incident, Problem, Change) used to provide Services.

4.9.2.2.7   Add new sites, equipment, and services into Successful Respondent Shared Services Systems (e.g., CMDB, Chargeback) used to provide Services.

4.9.2.2.8   Make changes to descriptors (e.g., name changes) associated with DIR and DIR Customers in all systems and reports.

4.9.3   Addition and Removal of Services

The Successful Respondent shall, at a minimum:

4.9.3.1   At the direction of DIR, develop and document in the Service Management Manual processes and procedures to support the addition and retirement of DIR services.

4.9.3.2   Perform a program management role to facilitate adding or removing DIR services, including:

4.9.3.2.1   Determine how the New Services are to be supported within the Successful Respondent and SCPs processes and systems.

Exhibit 2.1 Statement of Work   Page 103

4.9.3.2.2   Project manage DIR, DIR Customers, and SCPs in the activities related to the planning, solution development, and transition <u>into</u> operation for New Services.

4.9.3.2.3   Project manage DIR, DIR Customers, and SCPs in the activities related to the planning, solution development, and transition <u>out</u> for retired DIR Services.

4.9.3.2.4   Add New Services to Successful Respondent Shared Services Systems (e.g., Collaboration Portal, Incident, Problem, Change, etc.) used to provide Successful Respondent Services.

4.9.3.2.5   Add new sites, equipment, and services into existing Successful Respondent Shared Services Systems (e.g., CMDB, Chargeback) used to provide Successful Respondent Services.

4.9.3.2.6   Make changes to descriptors (e.g., name changes) associated with DIR and DIR Customers as needed to support the new or retired DIR Services.

4.10   Strategy Management

Strategy Management links the business demand with the supporting IT strategies and services along with service enhancement initiatives including a long-term strategy roadmap with timelines, and shorter-term technology plans which guide the annual improvement and budgeting process. Within this capability, DIR provides the leadership and coordination for the long-term strategy efforts, including but not limited to a long-term strategy roadmap, and Successful Respondent closely coordinates with DIR to support those efforts by coordinating the annual technology plan, the approval and communication of Standard Products, and coordinating the effective use and disposal of Equipment and Software.

4.10.1 Technology Planning

The Successful Respondent shall provide a process and ongoing program management for the establishment, currency, tracking, and publishing of a Technology Plan that incorporates input from DIR, DIR Customers, and SCPs and aligns with the governance processes.

The Successful Respondent shall, at a minimum:

4.10.1.1 Provide the platform to enable the aggregation of technical planning information from DIR, DIR Customers, Successful Respondent, SCPs, and CSPs as directed by TSS and DIR.

4.10.1.2 For MSI Services, proactively submit recommendations regarding new technology and automation to DIR for its review and approval.

4.10.1.3 For MSI Services, proactively seek to automate manual tasks associated with the Services including leading in the identification, solutioning and planning of MSI automation opportunities across the MSI and SCPs to increase automation, efficiencies and value, at a minimum, in the areas of service desk, service catalog, request workflow, MSI to SCP orchestration workflow, and data quality management, and document the agreed improvements in the Technology Plan, with deliverables implemented in accordance with the Annual Implementation of MSI Technology

Improvements deliverable in Exhibits 3.1 and 3.3.

4.10.1.4 Provide capacity to automate manual tasks associated with the Services including leading in the implementation of automation opportunities across the MSI and SCPs to increase automation and efficiencies.

4.10.1.5 Gather and incorporate the data and lessons learned from the operating environment that may impact DIR's and DIR Customers' plans.

4.10.1.6 Perform trend analysis from the resource consumption data to project future demand that may impact DIR's and DIR Customers' plans.

4.10.1.7 Evaluate market technology advances for Successful Respondent's tools and technologies that may provide DIR and DIR Customers greater capabilities or performance improvements.

4.10.1.8 Research and implement automated tools to improve Service Levels and/or performance of the computing environment. Tool selection will be in accordance with DIR and DIR Customers' standards and technical architectures.

4.10.1.9 Identify and propose technology evolutions that are likely to:

4.10.1.9.1 improve the efficiency and effectiveness of the Services (including cost savings) and DIR Shared Technology Services;

4.10.1.9.2 improve the efficiency and effectiveness of the processes, services and related functions performed by or for DIR and the DIR Customers;

4.10.1.9.3 result in cost savings or revenue increases to DIR and the DIR Customers in areas of their operations outside the DIR Shared Technology Services; and

4.10.1.9.4 enhance the ability of DIR and the DIR Customers to conduct their operations and serve their constituencies and customers faster and/or more efficiently than the then-current strategies.

4.10.1.10   Publish and promote technology plans with DIR Customers to ensure DIR Customer understanding, adoption, and business alignment.

4.10.1.11   Establish a Technology Planning Program as defined in the SMM that incorporates inputs from DIR, DIR Customers, and SCPs and aligns with established governance processes.

4.10.1.12   Monitor, and program manage the execution of Technology Planning responsibilities by SCPs and designated Third Parties.

4.10.1.13   Track and report on the completion progress of the Technology Plan.

Exhibit 2.1 Statement of Work   Page 105

4.10.2 Refresh and Technical Currency

The Successful Respondent will provide a process and ongoing program management for the establishment, currency, tracking, and publishing of a Refresh Plan that incorporates input from DIR, DIR Customers, and SCPs and aligns with the governance processes.

The Successful Respondent shall, at a minimum:

4.10.2.1 Establish an on-going Refresh Program that accomplishes the Refresh goals and coordinates the activities of DIR, DIR Customers, and SCPs, at the direction of the DIR.

4.10.2.2 Coordinate, monitor, and manage the execution of Refresh Responsibilities by SCPs and designated Third Parties.

4.10.2.3 Accommodate the timeframes and other requirements associated with Refresh, as well as the financial responsibility for the underlying assets, as provided in **Exhibit 4.2 Financial Responsibilities Matrix**.

4.10.2.4 Modify the Refresh timeframes and requirements during the Term, as directed by DIR, based on its business requirements, subject to the Change Control procedures.

4.10.2.5 Refresh Planning

The Successful Respondent shall, at a minimum:

4.10.2.5.1 In coordination with DIR, DIR Customers, and SCPs, develop and manage a continual plan for Refresh, as defined in **Exhibit 3.3, Critical Deliverables**, including:

4.10.2.5.1.1 Within one-hundred and twenty (120) days prior to DIR's annual planning process meetings, review the CMDB and produce a report that lists the assets that are due to be refreshed in the upcoming plan year, and provide such report to DIR's annual planning process.

4.10.2.5.1.2 Coordinate planning activities with DIR, DIR Customers, and SCPs.

4.10.2.5.1.3 The Successful Respondent and DIR will consider the usability of the assets and review alternatives to replace, release, consolidate, or retain the assets. Based on the results of this review, the Successful Respondent shall deliver the initial recommendations regarding such assets to DIR within thirty (30) days after the review.

4.10.2.5.1.4 For Successful Respondent-owned assets, Successful Respondent and DIR will mutually determine whether the Successful Respondent will replace an asset and the appropriate replacement date.

1. If Software Changes are required due to replacement of assets, Successful Respondent, in consultation with the DIR, will review alternatives for making changes to such Software.

2. Such replacement of the assets and Software will be at Successful Respondent's expense if the replacement is required to facilitate achievement of the agreed upon Service Levels or

Exhibit 2.1 Statement of Work   Page 106

because the asset is obsolete (i.e., replacement parts cannot be acquired or the asset has become unserviceable).

4.10.2.5.2 For DIR Customer owned and leased assets, based on the planning process outcome and direction established by DIR, the Successful Respondent shall provide to DIR a proposal for refresh of those assets (replacement at DIR Customer's expense).

4.10.2.6 Adhere to DIR's approved plan, and execute that plan utilizing established procurement processes, to initiate refresh and retirement activities.

4.10.2.6.1 Provide monthly reports one hundred eighty (180) days prior to lease expiration date showing assets to be refreshed with latest data.

4.10.2.6.2 Notify DIR monthly of all open agreements related to assets that are retired or will retire within one hundred eighty (180) days of the report date.

4.10.2.7 Track and report on the completion progress of asset Refresh.

4.10.2.8 Update and archive asset records after retirement.

4.10.3 Reference Architecture Standards and Standard Products

The Successful Respondent shall, at a minimum:

4.10.3.1 Coordinate, compile, recommend, and regularly (at least every ninety (90) days) update the Equipment and Software reference architecture standards describing shared infrastructure standards supporting delivery of services.

4.10.3.2 Coordinate, compile, recommend, and regularly (at least every ninety (90) days) update DIR Recommended Standard Products as determined using the Governance process (i.e., Operating System, Database, Middleware, job scheduling, etc.) describing equipment and software which align to program criteria recommended for use within the DIR Shared Technology Services.

4.10.3.3 Identify, track, and report through the Operational Intelligence System on DIR Customer use and non-use of Recommended Standard Products within the environment.

4.10.3.4 Collect and track all manufacturer end of life/out of support dates for deployed Equipment and Software in the environment.

4.10.3.5 Identify and report on the existing Equipment and Software in the environment along with manufacturer end of life / out of support plans and new offerings.

4.10.3.6 Make the reference architecture and standard products easily available on both the public facing portal and internal portal.

4.10.3.7 Report and facilitate Reference Architecture Standards and Recommended Standard Product decisions using the governance processes.

Exhibit 2.1 Statement of Work   Page 107

4.10.3.8 For approved Reference Architecture Standards and Recommended Standard Product changes, publish and make available the description of Recommended Standard Products to Authorized Users as requested by DIR.

4.10.3.9 Make the description of Reference Architecture Standards and Recommended Standard Products available on the Portal.

4.10.3.10 Provide support processes supporting alignment of the Recommended Standard Product list and Reference Architecture standards with DIR's strategic direction, technical architecture, and refresh strategy (i.e., Customer Technology Exception Processing)

4.10.3.11 Provide mechanisms and processes and procedures to capture feedback and business needs from DIR Customers as to changes in Recommended Standard Products and Reference Architecture standards.

4.10.3.12 Maintain the Recommended Standard Products list on a relational database system, containing links and integration with the Asset Inventory and Management System as necessary and appropriate with the database design approved by DIR.

4.10.3.13 Grant database access to DIR.

4.10.4 Reference Architecture and Standard Product Descriptions

The Successful Respondent shall, at a minimum:

4.10.4.1 Focus on broad, minimum requirements rather than on specific models or configurations (e.g., minimum processor type, minimum release level of Software, etc.).

4.10.4.2 Emphasize standards descriptions that are easily understood by Authorized Users. All Equipment and/or Software in use, which is within the refresh cycle approved by DIR and which may be changed from time to time based on technological change and/or business requirements, is considered Reference Architecture Standards and Recommended Standard Products.

4.10.4.3 Treat all Equipment and Software designated as standard as of the Commencement Date as Reference Architecture Standards and Recommended Standard Products; the Successful Respondent shall not treat any such Equipment or Software as out of compliance or unsupported until determined by the appropriate governance committee.

4.10.4.4 Present changes to Recommended Standard Products to the appropriate governance structure.

4.10.5 Reference Architecture and Standard Products Monitoring

The Successful Respondent shall, at a minimum:

4.10.5.1 Routinely educate DIR Customers on Reference Architectures and Recommended Standard Products, including bulletins about upgrade requirements, modification of

Exhibit 2.1 Statement of Work   Page 108

product support, compatibility issues, known problems with nonstandard products, etc.

4.10.5.2 Monitor and report on the environment for the introduction and use of nonstandard reference architectures and products within DIR.

4.10.5.3 Where an Authorized User is not utilizing Reference Architecture, take proactive steps to inform the Authorized User and include steps the Authorized User should take to obtain Reference Architecture.

4.10.5.4 Use and update the Asset Inventory and Management System to determine the potential use of nonstandard Equipment and/or Software by an Authorized User.

4.10.5.5 On at least a monthly basis, provide a report to DIR that lists all users that are not using Reference Architecture or Standard Products, and include the specific use of the nonstandard Equipment and/or Software.

4.10.5.6 Provide information to Authorized Users who could be affected by Governance decisions associated to Reference Architecture standards or Recommended Standard Products. This communication to Authorized Users must include the following:

4.10.5.6.1 Transmit the information via a broadcast email or post it on the Portal, or other means as approved by DIR, in advance of any Governance decisions which could impact DIR Customers' operations or Successful Respondent support responsibilities.

4.10.5.6.2 Provide information regarding the future Reference Architecture standards or Recommended Standard Products and/or the item in the Service Catalog that should be used as a replacement.

4.10.5.6.3 Provide information regarding who to contact or where to obtain additional information about the change to Reference Architecture or the Standard Product list.

5 OPERATIONS MANAGEMENT

5.1 Enterprise Event Management

Enterprise Event Management is an optional capability as elected by DIR.

Enterprise Event Management provides single management console visibility to operational health issues across the Services landscape and provides intelligent event analysis to support continuity Service performance. Events may include log messages, warnings or other alarms generated from the underpinning Services infrastructure and applications. Event monitoring is the responsibility of the SCPs and events are forwarded to the Successful Respondent.

The Enterprise Event Management function collects and aggregates forwarded events, correlates them, and incorporates them into the Successful Respondent Shared Services Systems (e.g., Incident Management System) for efficient management and resolution using the processes outlined in the Statement of Work. This functionality allows SCPs to provide full coverage of monitoring their respective services while the Successful Respondent filters and correlates events across SCPs and provides complete insight into the overall Services performance.

Exhibit 2.1 Statement of Work   Page 109

The effectiveness of Enterprise Event Management will be measured by the Key SLA Chronic Incidents, defined in **Exhibit 3.1 Service Levels Matrix** and **Exhibit 3.2 Service Level Definitions,** and by the Service Quality Key Performance Indicator defined in **Exhibit 3.4 Performance Analytics.**

5.1.1 Enterprise Event Management System

The Successful Respondent shall, at a minimum:

5.1.1.1 Provide and maintain an Enterprise Event Management System that will serve as the collector and correlation system for forwarded events provided by Successful Respondent and SCPs.

5.1.1.2 Integrate the Enterprise Event Management System with other systems for Service Management (e.g., Incident Management, Problem Management, Service Level Management, Asset Inventory and Management, Configuration Management, etc.).

5.1.1.3 Enable interfaces and integrate the Enterprise Event Management System with the event management systems of SCPs and designated CSPs.

5.1.1.4 Limit access to the Enterprise Event Management System to mutually agreed users who require access to the system.

5.1.1.5 Provide Successful Respondent personnel and authorized users with appropriate training in using the Enterprise Event Management System.

5.1.1.6 The Enterprise Event Management System shall at a minimum support the following:

    5.1.1.6.1 Consolidate alerts, alarms, logging information, and other monitored events from SCPs and CSPs.

    5.1.1.6.2 Configuration and automation of the processing of relationships between events across SCPs (referred to as correlations).

    5.1.1.6.3 Mapping of events to Incidents, Assets, and Configuration Items.

    5.1.1.6.4 Automatically initiating core processes specified in the Statement of Work (e.g., Incident Management).

    5.1.1.6.5 Collect forwarded events from SCPs and CSPs.

    5.1.1.6.6 Aggregate forwarded events from various systems.

    5.1.1.6.7 Collect and action alerts for near real-time event processing.

    5.1.1.6.8 Configure rules for identifying related events, events related to CIs and services and enrich the event for efficient subsequent processing and action.

    5.1.1.6.9 Configure rules for triggering Incidents and remediation actions.

    5.1.1.6.10 Implement and support dashboards for monitoring, analysis, and remediation of alerts.

    5.1.1.6.11 Provide eighteen (18) month history of events.

5.1.1.7 Maintain the Enterprise Event Management System to meet performance standards, to

Exhibit 2.1 Statement of Work   Page 110

maximize efficiency, and to minimize outages, as necessary.

5.1.1.8 Designate performance standards for the Enterprise Event Management System in the SMM.

5.1.1.9 Maintain, update, and implement the Enterprise Event Management System processes and procedures needed to recover from an outage or corruption within designated timeframes to meet DIR and DIR Customers' business requirements.

5.1.1.10 Test and implement Enterprise Event Management System changes, as approved by DIR.

5.1.1.11 Proactively provide capacity planning for the Enterprise Event Management System to prevent situations caused by lack of capacity (i.e., dataset or table space capacity events, full log files, etc.).

5.1.1.12 Correct situations caused by lack of Enterprise Event Management System capacity within designated timeframes (i.e., dataset or table space capacity events, full log files, etc.).

5.1.1.13 Provide Portal access to the Enterprise Event Management System for authorized DIR and Successful Respondent, including access to the data dictionary and user documentation.

5.1.2 Enterprise Event Management Operations

The Successful Respondent shall, at a minimum:

5.1.2.1 Coordinate and operate Enterprise Event Management activities across all functions, other SCPs, , and CSPs that provide services to DIR Customers.

5.1.2.2 Conduct regularly scheduled Enterprise Event Management meetings, included those associated with the requirements for governance as described in **Exhibit 1.2 Governance**.

5.1.2.3 Document and publish Enterprise Event Management meetings status reports to all relevant stakeholders.

5.1.2.4 Communicate and coordinate the Enterprise Event Management processes and policies within Successful Respondent's own organization, other SCPs, DIR, DIR Customers, and designated CSPs.

5.1.2.5 Provide on-going methods for training Successful Respondent staff, SCPs, DIR, and DIR Customers on the Enterprise Event Management Process.

5.1.2.6 Establish, operate, and manage Enterprise Event Management operations 24x7x365 to achieve the following objectives, scope, and principles to ensure the success of the Enterprise Event Management process:

Exhibit 2.1 Statement of Work   Page 111

    5.1.2.6.1   Collect forwarded events from SCPs and CSPs. Events may include:

        5.1.2.6.1.1 Aggregate forwarded events from various systems on a single console.

        5.1.2.6.1.2 Collect alerts for near real-time event processing

        5.1.2.6.1.3 Configure rules for identifying related events, events related to CIs and services and enrich the event for efficient subsequent processing and action.

        5.1.2.6.1.4 Configure rules for triggering Incidents and remediation actions.

        5.1.2.6.1.5 Implement and support dashboards for monitoring, analysis, and remediation of alerts.

        5.1.2.6.1.6 Provide eighteen (18) month history of events.

5.2   Data Quality Management

The Successful Respondent shall provide a platform to collect data internally, from SCPs and Third Party Vendor(s) enabling automated intake and analysis of hardware, software, and application integrity in support of the Asset Inventory and Management and Configuration Management processes. The Successful Respondent shall develop processes and integrate both SCP and Successful Respondent data to ensure quality and accurate data for all DIR Shared Technology Services.

The effectiveness of Data Quality Management will be measured by the accuracy of financial invoices, Operational Intelligence and service delivery outcomes.

The Successful Respondent shall, at a minimum:

5.2.1.1   Enable automated collection of hardware and software assets and configuration information for use in the core processes (e.g., Asset Inventory and Management, Configuration Management, Operational Intelligence).

5.2.1.2   Provide an integration platform allowing the configuration of workflow processes and interfaces to electronically collect data from multiple sources (e.g., flat files, databases, URLs) normalize the raw data, analyze data integrity issues and reconcile the data to the CMDB.

5.2.1.3   Enable automated collection of public cloud billing information for use in the IT Financial Management process (e.g., AWS cost and usage report extraction).

5.2.1.4   Provide a workflow process and integration platform to enable the Successful Respondent to configure workflow processes and interfaces to electronically collect public cloud billing information as available by the CSP.

5.2.1.5   Enable the information to be reconciled and integrated into the IT Financial Management process.

5.2.1.6   Enable automated collection of public cloud configuration, performance and billing information for use in the Incident Management, Asset Inventory and Management, Configuration Management, Operational Intelligence, Financial Management and

Service Level Management process (e.g., views of cloud compute, network and storage).

5.2.1.7   Provide a workflow process and integration platform to enable the Successful Respondent to configure workflow processes and interfaces to electronically collect public cloud configuration and performance information as available by the particular public CSP.

5.2.1.8   Enable the information to be reconciled and integrated into the Successful Respondent processes.

5.2.1.9   Evaluate accuracy and quality of data, implementing system or process improvements where necessary.

5.3   Workflow Orchestration

Provide and manage a platform with process workflow automation across Successful Respondent, SCPs, and CSPs to enable increased self-service, automated issue remediation, automated Service Request resolution and digital governance as required (e.g., Service Catalog Management, Incident Management, Request Management, and Service Level Management processes).

The Successful Respondent shall, at a minimum:

5.3.1.1   Enable efficiencies, automation and self-service processing of Service Catalog Management, Incident Management, Request Management and Change Management activities (e.g., Incident routing to SCPs for auto healing, Digital CAB workflow processing).

5.3.1.2   Provide an extensible process and integration platform to enable the Successful Respondent to configure electronic workflow processes and interfaces to automate work activities across the Successful Respondent, DIR Customers, SCPs and CSPs (e.g., personnel onboarding and off boarding, change request review and approval routing, password reset, automated Incident remediation, etc.).

5.3.1.3   Enable the Service Catalog, Request Management, Change Management, and Incident Management processes to leverage the self-service platform for use by DIR Customers, Successful Respondent, or SCPs.

5.3.1.4   For integrations between MSI systems and SCP/CSP Systems, work with the SCPs and CSPs to define, maintain, and document standard interface specifications, as approved by DIR, including the integration methods (e.g., extract, API), data values, formats, and frequency.

5.3.1.5   For integrations where DIR-approved interface specifications cannot be supported by an SCP, escalate to DIR with full explanation of the issue and provide suggested mitigations and their corresponding implications (e.g., lower frequency file upload interface).

Exhibit 2.1 Statement of Work   Page 113

NOTE: The SCP or CSP will be responsible for developing and supporting the SCP or CSP-side of the interface within SCP/CSP systems as well as jointly working with MSI for testing and maintenance of integrations.

<div style="background-color:#333; color:white;">

5.4   Cloud Management

</div>

The Successful Respondent will provide and manage a platform to enable automated public and private cloud workflow orchestration across the Successful Respondent, through SCPs and to public CSP, as well as, public cloud workflow orchestration from the Successful Respondent direct to public CSPs. This capability enables self-provisioned services, automated and orchestrated by the Successful Respondent, to expedite speed to value and increase customer satisfaction as required in the Service Catalog Management, Request Management, and Incident Management processes.

5.4.1   Cloud Management Systems and Processes

The Successful Respondent shall, at a minimum:

5.4.1.1   Provide direct interfacing capabilities to support efficient self-service provisioning and management of public cloud (e.g., AWS server and storage, Azure server and storage) services.

5.4.1.2   Provide an extensible process and integration platform for Successful Respondent to configure electronic workflow processes and interfaces to perform public cloud management activities as available by the particular public CSP (e.g., cloud account configuration, order and manage VM instance, start/stop instances, allocate/release IP addresses, allocate storage, increase CPU, or memory, etc.).

5.4.1.3   Enable the Service Catalog, Request Management, and Incident Management Systems and processes to leverage the self-service platform for use by DIR Customers, Successful Respondent, or SCPs.

5.4.1.4   Implement, manage, and maintain all Application Program Interfaces (APIs) required to keep the Service Catalog current and orchestrate Service provisioning.

5.4.1.5   Provide self-service provisioning of on premise services (e.g., VMware vBlock server) in the DCS consolidated data centers.

5.4.1.6   Provide an extensible process and integration platform to enable the Successful Respondent to configure electronic workflow processes and interfaces to perform on premise compute and storage management activities as available by the particular SCPs (e.g., account configuration, reboot instances, allocate/release IP addresses, allocate storage, increase CPU or memory, etc.).

5.4.1.7   Design, develop, and support the integration of the Successful Respondent Shared Services Systems with the SCP orchestration tools, including:

5.4.1.7.1   With the Successful Respondent Service Catalog for order information and status of order and pricing updates,

---

Exhibit 2.1 Statement of Work   Page 114

     5.4.1.7.2 With the Successful Respondent Financial System for billing data including usage and pricing,

     5.4.1.7.3 With the Successful Respondent Incident and Request System for fulfillment ticket status,

     5.4.1.7.4 With the Successful Respondent Asset Inventory and Management System and CMDB for inventory and CI status.

5.4.1.8 Design, develop, and update the IT Financial Management System to enable invoicing and chargeback for cloud services.

6 TRANSITION

6.1   Transition Requirements

6.1.1 General

The Successful Respondent shall:

6.1.1.1 Provide sufficient staff, tools and processes to ensure all Services successfully transition from the incumbent MSI without service degradation to Customers.

6.1.1.2 Ensure SCPs successfully transition to Successful Respondent tools and processes by Commencement without service degradation to DIR Customers.

6.1.1.3 Develop a detailed Transition Plan including the Successful Respondent's approach to transitioning Services from the Incumbent MSI and the existing Texas.gov Service Provider. The Transition Plan should include, at a minimum, all systems, processes, data (e.g., Incumbent ITSM data) and reporting that is required to transition from the Incumbent MSI. See **Exhibit 3.3 Critical Deliverables** for further requirements.

6.1.1.4 Provide twenty-four (24) months of Incumbent-provided ITSM data in a read-only format.

6.1.1.5 Implement and provide public cloud billing interfaces to achieve public cloud billing requirements are described in Exhibit 2.1, section 5.2.1 by September 1, 2018.

6.1.1.6 Implement and provide public cloud provisioning to achieve requirements described in Exhibit 2.1, sections 5.2 Data Quality Management and 5.4 Cloud Management, by September 1, 2020, or as directed by DIR.

6.1.2 People and Training

6.1.2.1 The Successful Respondent shall provide sufficient staffing to accomplish Transition requirements. These staff must be sufficiently trained on the Successful Respondent's contractual requirements and the Successful Respondent's proposed solution prior to commencing Transition activities.

6.1.2.2 The Successful Respondent shall be responsible for all knowledge transfer from the

Incumbent MSI.

6.1.2.3   The Successful Respondent shall train DIR, DIR Customers, and SCPs on the Successful Respondent's systems, processes and Services prior to Commencement.

6.1.3   Existing Service Component Provider Integration

MSI Services are critical to providing DIR Customers with seamless service delivery across multiple SCPs. SCPs for DCS, MAS, and MSS are existing SCPs integrated with the incumbent MSI. Additional SCPs may be added throughout the course of the Contract.

6.1.3.1   The Successful Respondent shall ensure the successful transition and integration of all SCPs.

6.1.3.2   The Successful Respondent shall identify all integration points of the Successful Respondent's solution that require existing SCPs to make changes and notifying each SCP of the required changes at least ninety (90) days prior to Commencement.

6.1.3.3   The Successful Respondent shall train SCPs on the Successful Respondent's Services, systems, and SMM processes, focusing on the changes from the incumbent MSI Services.

6.1.3.4   The Successful Respondent shall create a schedule for all SCPs to complete integration changes and ensure the accuracy of those changes.

6.1.3.5   The Successful Respondent shall manage the integration transition tasks and schedule.

6.1.3.6   The Successful Respondent shall test the accuracy of all integration points prior to Commencement.

6.1.3.7   The Successful Respondent shall collaborate with SCPs to resolve any identified issues.

6.1.4   Texas.gov Integration

During the Successful Respondent's Transition, the Texas.gov service delivery model will be transitioning from a public/private partnership with a single vendor to an outsourced delivery model with multiple SCPs.

6.1.4.1   The Successful Respondent shall ensure Texas.gov SCPs are integrated into the Successful Respondent's Services.

6.1.4.2   The Successful Respondent shall conduct knowledge transfer of integration services performed by the incumbent Texas.gov provider and identify integration points with the new Texas.gov SCPs who will commence services at the same time as the Successful Respondent.

6.1.4.3   The Successful Respondent shall train the new Texas.gov SCPs on the Successful Respondent Services and service model in its entirety.

Exhibit 2.1 Statement of Work   Page 116

6.1.4.4 The Successful Respondent shall create a schedule for the Texas.gov SCPs' integration tasks that is coordinated with the SCPs' own service implementation schedule.

6.1.4.5 The Successful Respondent shall manage the Texas.gov integration tasks and schedule.

6.1.4.6 The Successful Respondent shall test the accuracy of all integration points prior to Commencement.

6.1.4.7 The Successful Respondent shall collaborate with SCPs to resolve any identified issues.

6.1.5 Configuration Management Data Base (CMDB)

An accurate CMDB is critical to the successful delivery of services for all SCPs. The Successful Respondent is responsible for creating and maintaining an accurate CMDB.

6.1.5.1 The Successful Respondent shall develop a plan to transition the Incumbent MSI's CMDB, including tasks to reconcile and validate data accuracy.

6.1.5.2 The Successful Respondent shall implement data quality management systems to ensure ongoing CMDB data accuracy.

6.1.5.3 The Successful Respondent shall deliver to DIR the results of the automated CMDB population and reconciliation, demonstrating accurate data has been populated in order to enable accurate operational services, reporting and financial invoices, according to the schedule defined in **Exhibit 3.3, Critical Deliverables**.

6.1.6 Service Management Systems

6.1.6.1 The Successful Respondent shall identify, schedule, and deploy all software and systems that will transition from the Incumbent MSI to the Successful Respondent.

6.1.6.2 The Successful Respondent shall identify, schedule, and deploy all new software and systems required to deliver Successful Respondent Services.

6.1.6.3 The Successful Respondent shall provide documentation demonstrating each service level measurement was tested and validated for accuracy, as defined in **Exhibit 3.3, Critical Deliverables**.

6.1.6.4 Ensure all service management systems accurately and appropriately support all service operations requirements specified in the Statement of Work.

6.1.6.5 Produce all one-time Critical Deliverables associated with Transition, as defined in **Exhibit 3.3, Critical Deliverables**.

6.1.7 Financial Management

6.1.7.1 The Successful Respondent shall seamlessly transition SCP invoicing and DIR Customer Chargeback billing from the Incumbent MSI.

Exhibit 2.1 Statement of Work   Page 117

6.1.7.2 The Successful Respondent shall ensure all historical data is transitioned accurately to the Successful Respondent's IT Financial Management tool.

6.1.7.3 The Successful Respondent shall test all SCP billing feeds to ensure accuracy and provide documentation demonstrating accurate testing.

6.1.7.4 The Successful Respondent shall validate accurate invoicing and DIR Customer Chargeback prior to Commencement.

6.1.8   Project Management

6.1.8.1 The Successful Respondent shall provide project management over all Successful Respondent Service Transition and SCP integration Transition.

6.1.8.2 The Successful Respondent shall provide routine reports and communication on Transition status to DIR and SCPs, as directed by DIR.

6.1.8.3 The Successful Respondent shall meet with DIR and SCPs to report on Transition activities, status, issues and risks.

6.1.8.4 The Successful Respondent shall resolve issues collaboratively with DIR and SCPs in order to meet Transition schedule.

6.1.8.5 The Successful Respondent shall regularly communicate the status of Transition, training, and changes to DIR Customers.

7   OPERATIONS

7.1   Staffing

7.1.1   The Successful Respondent shall, at a minimum:

7.1.1.1 Adjust and provide sufficient staffing to meet Contract requirements including Service Level Agreements (SLAs) and oversight requirements.

7.1.1.2 Notify DIR of any changes to Key Personnel a minimum of thirty (30) DIR Business Days prior to change**s.**

7.1.1.3 Provide the resume(s) of proposed replacement Key Personnel to DIR for review, possible interview, and approval. Replacement Key Personnel shall have qualifications that are equal to or exceed those of the person being replaced. Approval of Key Staff is at the sole discretion of DIR.

7.1.1.4 Provide an organization chart for review and approval by DIR. The proposed organization chart shall at a minimum, identify all Key Personnel including a representative responsible for each functional service delivery area and define clear lines of authority and accountability for delivery of services, issue resolution and financial management. DIR at its sole discretion may require the replacement of any

Exhibit 2.1 Statement of Work   Page 118

staff, including Key Personnel, with written notice to the Successful Respondent.

7.1.1.5   In the Service Management Manual (SMM), identify its issue management and escalation process through its organization.

7.1.1.6   Provide Key Personnel including, but not limited to, the following functional areas:

    7.1.1.6.1   Account Director with overall financial and service delivery accountability for the MSI contract.

    7.1.1.6.2   MSI Chief Technology Officer for the account with overall accountability to provide cross-functional platform strategy and architecture leadership designed to drive seamless and automated services throughout the service lifecycle of ordering, provisioning/updating and billing, and across all providers in the Shared Technology Services ecosystem.

    7.1.1.6.3   Service Delivery Director with overall accountability for delivery of the Successful Respondent's requirements and DIR's Shared Services.

    7.1.1.6.4   Business Intelligence Director with overall accountability for all data, reporting and business intelligence.

    7.1.1.6.5   Finance Director with overall accountability for all chargeback, invoicing, billing disputes, pricing, and financial reporting.

    7.1.1.6.6   Transition Director with overall accountability for delivery of the Successful Respondent's transition through completion and DIR acceptance of all Transition deliverables.

    7.1.1.6.7   Customer Relationship Management personnel with overall management of DIR Customer strategic and tactical Shared Service demand, consumption and performance.

    7.1.1.6.8   Other, as the Successful Respondent deems key to the fulfillment of its contract obligations.

7.1.1.7   Key Personnel shall be dedicated full time to the Successful Respondent's contract, not leveraged to other accounts.

7.1.1.8   Key Personnel shall be committed for twenty-four (24) months minimum from commencement of the contract unless stated otherwise. After twenty-four (24) months, replacement Key Personnel shall be committed for a minimum of twelve (12) months.

7.1.1.9   The Successful Respondent shall provide a table with information on Key Personnel, including name, title, functional area, and commitment timeframe. The table shall be maintained by the Successful Respondent and provided to DIR upon request.

7.2   Safety and Security

7.2.1   The Successful Respondent shall, at a minimum:

7.2.1.1   Adhere to the then-current safety and security policies, rules, procedures and regulations established by the State and DIR, and each DIR Customer with respect to such DIR Customer's data and facilities.

Exhibit 2.1 Statement of Work   Page 119

7.2.1.2   Adhere to DIR and DIR Customer's then-current "Security Rules," as published in Chapter 202, Information Security Standards of the Texas Administrative Code.

7.2.1.3   Comply with the policies defined by state and federal regulations, including the FBI Criminal Justice Information Services (CJIS) requirements.

7.2.1.4   DIR and DIR Customers comply with National Institute of Standards and Technology (NIST) Federal standards and related NIST 800 series Special Publications (SP) and Federal Information Processing Standards (FIPS) standards. Where there is a conflict between NIST, FIPS and 1 TAC Chapter 202 rules and security controls, the 1 TAC Chapter 202 takes precedence.

7.2.1.5   Implement a SMM that includes Security Incident Response, the Texas Cybersecurity Framework, Texas Administrative Code Chapter 202, and NIST-based security controls and processes.

7.2.1.6   Establish the security program to tie to the Texas Cybersecurity Framework and integrate with the DIR Governance Risk and Compliance program.

7.3   Disposal of Data and Confidential Information

DIR and DIR Customers fall under, and the Successful Respondent shall comply with, those federal and State laws that address the proper handling, securing, and disposing of data in both physical and electronic form. Some examples include the DIR Control Standards Catalog (including the requirements and procedures outlined in MP-6 addressing the disposal of data processing equipment under Chapter 403.278, Texas Government Code (between institutions of higher education or state agencies) and Chapter 2175, Texas Government Code (for all other transactions)), the Internal Revenue Code ("IRC"), the Fair and Accurate Credit Transactions Act ("FACTA"), the Family Educational Rights and Privacy Act ("FERPA"), the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the Gramm-Leach Bliley Act and the Federal Information Security Management Act ("FISMA").

7.3.1   The Successful Respondent shall, at a minimum:

7.3.1.1   Sanitize all types of electronic media and non-volatile memory prior to disposal or release for reuse.

7.3.1.2   Provide secure erasure of data from products and/or services (e.g., computers, switches/routers, telephones, printers, fax machines, scanners, multifunction devices, etc.) prior to final disposition outside the secure data center environment. Approved methods for media and memory sanitization are listed in the NIST Special Publication 800-88, Guidelines for Media Sanitization.

7.3.1.3   Document and verify media sanitization and disposal actions.

7.3.1.4   Comply with and adhere to these and all other applicable federal and state guidelines.

Exhibit 2.1 Statement of Work   Page 120

7.4 Security Clearances

7.4.1 The Successful Respondent shall ensure, at a minimum:

7.4.1.1 Successful Respondent personnel have received security clearance and successfully complete a background and criminal history investigation prior to performing contract functions or accessing DIR, DIR Customer Facilities, Systems, Networks, or Data.

7.4.1.2 Criminal history background checks are conducted per Texas Government Code (TGC) Subchapter F, Section 411.1404 and will be in compliance with the then-current versions of the FBI CJIS Security Policy and the FBI CJIS Security Addendum. In addition, an annual background check re-verification is required. The Successful Respondent shall notify DIR of compliance with the initial criminal history background check and the annual re-verification.

7.4.1.3 Background and criminal history background checks are performed by the Texas Department of Public Safety, Texas Department of Criminal Justice, and the Texas Department of Family and Protective Services. Other DIR Customers may require additional levels of compliance as per agency regulations and policies.

> **NOTE:** Successful Respondent is responsible for any costs associated with the criminal history background check process.

7.4.2 The Successful Respondent shall:

7.4.2.1 Establish a process that facilitates the timely submission and resolution of the criminal history background checks, including but not limited to using digital methods to submit necessary criminal history background check requirements.

7.4.2.2 Establish and document processes and procedures for complying with the security clearance requirements, to include on-boarding and off-boarding processes and procedures.

7.4.2.3 Ensure that any Successful Respondent personnel with logical or physical access to DIR Facilities or Data has successfully obtained the appropriate security clearance.

7.4.2.4 Ensure that any Successful Respondent personnel that has not completed the security clearance requirements are escorted at all times while at DIR and the DCS consolidated data centers.

7.4.2.5 Implement processes and procedures for tracking clearances for all Successful Respondent personnel and other SCPs.

7.4.2.6 Ensure that there is auditable tracking of access granted, logical security clearances and access revocations for all Successful Respondent personnel.

7.4.2.7 Provide training and awareness for SCPs' employees and Subcontractors regarding compliance with the Security Program, DIR, and DIR Customer security policies, practices, and procedures, including DIR Customer unique security training. The initial

Exhibit 2.1 Statement of Work   Page 121

security awareness training and signed non-disclosure agreement must be completed prior to access to information systems and is required annually thereafter. The Successful Respondent shall provide documentation of such training to DIR.

7.4.2.8 Track which individuals have been trained on the Security Program, DIR, and DIR Customer security policies and procedures as appropriate.

7.4.2.9 Report on the security clearances at DIR and DIR Customer request.

7.4.2.10 Provide physical and logical access reports as requested by DIR and DIR Customers.

7.5   Systems Incident and Request Management

The Successful Respondent will support the resolution of Incidents and Requests relating to the Successful Respondent-provided Services.

7.5.1   The Successful Respondent shall, at a minimum:

7.5.1.1 For Successful Respondent assigned Incidents and Requests, perform all resolution responsibilities in accordance with the SMM, knowledge database documents, and configuration database(s), including the following:

  7.5.1.1.1 Provide Level 1 Support, Level 2 Support, and Level 3 Support.
  7.5.1.1.2 Update the progress of an Incident's resolution within the Successful Respondent Shared Services Systems through to final closure.
  7.5.1.1.3 Verify that all records (e.g., asset inventory, configuration management records) are updated to reflect completed/resolved Incidents.
  7.5.1.1.4 Document solutions to resolved Incidents in Successful Respondent managed central knowledge base. Accurately update all information pertinent to Incident ticket including general verbiage, codes, etc.
  7.5.1.1.5 Determine wherever possible whether an Incident should initiate a Problem investigation (e.g., whether preventive action may be necessary to avoid Incident recurrence) and, in conjunction with the appropriate support tier, raise a Problem record to initiate action.
  7.5.1.1.6 Conduct follow-up with Authorized User who reported the Incident to verify that the Incident was resolved to their satisfaction.

7.6   Operations Documentation

All documentation maintained by the Successful Respondent will be subject to approval by DIR and will conform to the documentation standards and format agreed upon between DIR and Successful Respondent. The Successful Respondent will develop documentation in accordance with the requirements in **Exhibit 3.3 Critical Deliverables**.

The Successful Respondent shall, at a minimum:

7.6.1.1 Ensure that Successful Respondent-specific operations documentation is up to date,

Exhibit 2.1 Statement of Work   Page 122

accurate and posted in the SMM.

7.6.1.2 Develop and maintain documentation on all Operations procedures, services, Equipment, and Software for which Successful Respondent is responsible (e.g., project kick-off procedure, backup procedures, service desk scripts by agency, product ordering procedure, proposal formation procedure).

7.6.1.3 Document Application requirements that affect Operations, along with procedural information and contact information for each Application.

7.6.1.4 Make all documentation available electronically, as requested by DIR.

7.6.1.5 Validate documentation regularly for completeness and accuracy, and verify that all documentation is present, organized, readable, and updated.

7.6.1.6 Participate in the reporting of validation findings to DIR on a regular basis, and where it is determined that documentation is inaccurate (e.g., erroneous or out of date), correct and replace such documentation.

7.6.1.7 Update the SMM according to the schedule described in **Exhibit 3.3 Critical Deliverables**.

7.7 License Management and Compliance

Where Successful Respondent is financially responsible for Software associated with the Services, the Successful Respondent shall, at a minimum:

7.7.1.1 Comply with all Software license requirements by monitoring and validating Software use.

7.7.1.2 Proactively monitor the use of the Software in order to maintain strict compliance, including:

7.7.1.3 Immediately notify and advise DIR of all Software license compliance issues.

7.7.1.4 Provide the Software and acquire the correct number of the licenses to be compliant with Successful Respondent's Third Party Vendor requirements.

7.7.1.5 Monitor the Equipment for the presence of any unauthorized or non-standard Software.

7.7.1.6 Track license counts and associations.

7.7.1.7 Manage and track security certificates used to secure confidential sessions (e.g., SSL) for Internet and Intranet transactions and communications, including processes and procedures for renewals.

7.7.1.8 To the extent enabled by Successful Respondent Shared Services System, perform the following activities:

Exhibit 2.1 Statement of Work   Page 123

7.7.1.8.1 Define and check for particular Software signatures.

7.7.1.8.2 Monitor the use of Software developed by Successful Respondent application development groups.

7.7.1.8.3 Check the presence and version of Software installed on a particular device and record in the asset management system.

7.7.1.9 Provide reporting of license information and compliance to DIR, at least quarterly or as directed by DIR.

7.7.1.10 File and track Software license agreements and associated license keys, including processes and procedures for renewals; associate with CI in the CMDB.

7.8 Vulnerability Management

The Successful Respondent shall, at a minimum:

1. Establish and manage a NIST-based vulnerability management program for Successful Respondent-provided systems.

2. Ensure vulnerability scans are run monthly and address vulnerabilities.

3. Record Successful Respondent identified vulnerabilities in the DIR (GRC) tool (Currently SPECTRIM) using an agreed interface (e.g., .csv SFTP).

4. Track status of identified vulnerabilities and risk mitigation actions, and reporting, of identified vulnerabilities, where vulnerability levels to be tracked are specified and defined in the SMMs.

5. Provide DIR with a monthly status of Successful Respondent vulnerabilities found along with the remediating actions.

6. On a quarterly basis perform a review of all users assigned access to Successful Respondent systems and confirm access validity providing report to DIR.

7.9 Network Connectivity

The Successful Respondent shall, at a minimum:

7.9.1.1 If Successful Respondent chooses to implement some portion of the Services in facilities outside of the Consolidated Data Centers (e.g., disaster recovery sites, service delivery centers, etc.), Successful Respondent shall provide the network connections from those locations to the Consolidated Data Centers.

7.9.1.2 Coordinate with the Network SCP for network connectivity within the Consolidated Data Centers for provision of the Services.

7.9.1.3 Provide the network connections between the Consolidated Data Centers, where Successful Respondent has some portion of the Services that require connections between the Consolidated Data Centers (e.g., data replication for disaster recovery, backup to a remote location, etc.).

Exhibit 2.1 Statement of Work
Page 124

7.9.1.4   For the network connections provisioned by Successful Respondent as part of its solution:

    7.9.1.4.1   Manage and support the network connections (e.g., WAN circuits).

    7.9.1.4.2   Ensure there is adequate bandwidth to support the full use of Services.

    7.9.1.4.3   Coordinate with the Network SCP to ensure proper connectivity between Successful Respondent's transport and the Consolidated Data Centers LAN.

    7.9.1.4.4   Ensure the network connections in support of the Services adhere to the Government security requirements and in accordance with DIR policy

7.10   Shared Services Systems Release Management

1. The Successful Respondent shall perform integrated pre-production testing, for all Successful Respondent supported Software (e.g., ITSM, Chargeback, Portal).

2. The Successful Respondent shall use the Release Management processes, policies, and procedures to communicate and coordinate updates to the Successful Respondent Systems across SCPs, DIR, and DIR Customers.

7.11   Equipment and Software Maintenance

Specific operational responsibilities for various categories of Software are described in the Statement of Work, and in **Exhibit 4.2 Financial Responsibility Matrix**. Where Successful Respondent is financially responsible for the underlying Equipment or Software, Successful Respondent is responsible for the coordination of, tracking, and escalation necessary to ensure Successful Respondent meets commitments related to the delivery of Services to DIR.

The Successful Respondent shall, at a minimum:

7.11.1.1 Ensure that all Systems managed by the Successful Respondent are protected against unauthorized access. This includes:

    7.11.1.1.1 Installation of the latest software patches from a verifiable vendor.

    7.11.1.1.2 Disable any unnecessary services.

    7.11.1.1.3 Install and update antivirus Software in all environments.

    7.11.1.1.4 On a quarterly basis, perform a review of all users assigned access to Successful Respondent systems and confirm access validity providing report to DIR.

7.11.1.2 Ensure all systems and applications that the Successful Respondent uses to support DIR and DIR Customers are in a supported and secure state.

7.11.1.3 Ensure that all Software used in fulfillment of this Agreement complies with DIR's and the DIR Customers' security policies, procedures, rules and regulations in accordance with the terms of the Agreement, including those documented in the SMM.

7.11.1.4 Coordinate and manage all Third Parties that provide maintenance-related support for Equipment and Software used in conjunction with the Services.

Exhibit 2.1 Statement of Work   Page 125

7.11.1.5 Perform all maintenance of Equipment and Software in accordance with Change Management procedures, and schedule this maintenance to minimize disruption to DIR's and DIR Customers' business.

7.11.1.6 Provide or arrange for qualified Third Parties to provide maintenance for such Equipment and Software.

7.11.1.7 Provide such maintenance as necessary to keep the assets in good operating condition and in accordance with the manufacturer's specifications, or other agreements as applicable, so that such assets will qualify for the manufacturer's standard maintenance plan upon sale or return to a lessor.

7.11.1.8 At all times, provide maintenance for Equipment and Software as necessary to meet specified Service Levels, including:

7.11.1.8.1 Providing maintenance for Equipment and Software not under maintenance contracts.

7.11.1.8.2 Provide commercially reasonable efforts to maintain Equipment and Software no longer supported by the OEM.

7.11.1.9 For Third Party maintenance contracts, Successful Respondent responsibilities shall include:

7.11.1.9.1 Administer and manage the contract on behalf of DIR as applicable.

7.11.1.9.2 Notify DIR in advance about maintenance contracts that are about to expire.

7.11.1.9.3 Recommend modifications to the services during Third Party maintenance contract renewal.

7.12   Software Support

Specific operational responsibilities for various categories of Software are described in the Statement of Work, and in **Exhibit 4.2 Financial Responsibility Matrix**.

7.12.1 Installation, Upgrades and Changes

The Successful Respondent shall, at a minimum:

7.12.1.1 Install, upgrade, and change all Software as required and in accordance with DIR technical architecture standards.

7.12.1.2 Interface with DIR, SCP, and Third Parties to promote the compatibility of Software products.

7.12.1.3 Unless otherwise directed by DIR, install, upgrade, and change Software to prescribed release levels, maintaining software currency prescribed in **Exhibit 4.2 Financial Responsibility Matrix** and make available all enhancements provided for in the Statement of Work.

7.12.1.4 Install Third Party-supplied corrections for Third Party Software problems, which

Exhibit 2.1 Statement of Work   Page 126

include installation of Third Party-supplied Software patches as required.

7.12.1.5 Give written notice to DIR at least ninety (90) days in advance of all upgrades and Software changes that are planned to occur in the following calendar quarter. DIR and SCPs will mutually agree in writing on the timing for the implementation of upgrades.

7.12.1.6 Coordinate testing, installation, customization, and support of Software with Application Development and Maintenance (ADM) personnel, DIR, and SCPs as required.

7.12.1.7 Establish designated patching windows that are coordinated with DIR Customer and SCP schedules.

7.12.1.8 Observe DIR Change Management procedures while implementing changes, upgrades, or enhancements.

7.12.1.9 For any changes, upgrades, or enhancements, advise DIR and SCPs of any additional Equipment, network, environmental, or other requirements needed during integration testing and/or otherwise known to be necessary for the implementation.

7.12.1.10   Provide reports, at least monthly, on software upgrades applied, including patching to DIR.

7.12.1.11   Provide monthly reports of upcoming software releases, software renewals and end-of-support notices to DIR and affected SCPs, at least one hundred eighty (180) days prior to expirations date.

7.12.2 Software Support

The Successful Respondent shall, at a minimum:

7.12.2.1 Maintain documentation on Software that reflects the complexity and diversity of the environment and that enhances the Software support process (e.g., installation, maintenance, interfaces, active processes).

7.12.2.2 Maintain a library of documentation that identifies the Software required to support the Services and the operational support procedures associated with the Software.

7.12.2.3 Maintain, update and ensure currency in the Configuration Management process for all software.

7.12.2.4 Support all Successful Respondent-provided Software as required and in accordance with DIR's technical architecture standards.

7.12.2.5 Support Software at prescribed release levels or as directed by DIR.

7.12.2.6 Correct/make changes to Software as required.

7.12.2.7 Provide Authorized Users with Software support, advice, and assistance.

Exhibit 2.1 Statement of Work   Page 127

7.12.2.8 Review all Software conversion, migration, and upgrade plans with, DIR, SCPs, and DIR Customers.

7.12.2.9 Provide a software currency review on an annual basis and provide the report to DIR along with the mitigating activities required to address the security problem in accordance with applicable DIR Standards.

7.12.3 Malicious code or unauthorized code Protection

The Successful Respondent shall, at a minimum:

7.12.3.1 Install, update, operate, and maintain malware protection or unauthorized code protection Software on all Equipment used to deliver or support the Services (e.g., servers, laptops) in compliance with this document, TAC 202 and applicable Federal policies.

7.12.3.2 Maintain subscription to the anti-malicious code or unauthorized code Software support in order to proactively receive malicious code or unauthorized code engine and pattern updates.

7.12.3.3 Install updates, in accordance with Change Management, to malicious-protection Software as needed or as directed by DIR or DIR Customer, no later than twenty-four (24) hours after such updates are made available to Successful Respondent (or qualified Third Parties selected by Successful Respondent) and approved by DIR.

7.12.3.4 Perform scans for malicious code or unauthorized code on all emails, including email attachments.

7.12.3.5 Provide for 24x7 security monitoring and reporting on Security events on Successful Respondent systems used in support of this account.

7.12.3.6 Upon detection of malware or unauthorized code, take immediate steps to notify DIR, Customer and the Service Desk in compliance with guidelines contained in this document and the SMM, as well as to:

7.12.3.6.1 Assess the scope of damage.

7.12.3.6.2 Arrest the spread and progressive damage from malware or unauthorized code.

7.12.3.6.3 Eradicate malware or unauthorized code.

7.12.3.6.4 Restore all data and Software to its original state.

7.12.3.7 Monitor and scan diskettes or hard drives or other temporary storage devices (such as USB memory sticks, PCMCIA flashcards, FireWire hard drives, etc.) for malware or unauthorized code upon demand.

7.12.3.8 Develop any plans necessary to provide malware protection or unauthorized code protection.

7.12.3.9 Provide consulting services for malware protection or unauthorized code protection.

Exhibit 2.1 Statement of Work   Page 128

7.12.3.10   Respond to malware or unauthorized code Incidents.

7.12.3.11   Provide proactive alerts to Authorized Users relative to current malware or unauthorized code threats either specific to DIR's environment, encountered in Successful Respondent's environment, or based on industry information.

7.12.3.12   Provide additional temporary resources in the event of a major computer malware or unauthorized code outbreak so DIR's and DIR Customers' performance does not degrade because of an unavailability of Successful Respondent resources.

7.12.3.13   Provide daily and monthly reports, broken out by DIR Customer and in compliance with DIR and DIR Customer policies that contain a summary of the number of malware or unauthorized code detected and cleaned, as well as a list of malware caught.

7.13   Services Business Continuity and Disaster Recovery

The Successful Respondent has full responsibility for their Business Continuity plans and Disaster Recovery plans, testing and recovery activities for the Successful Respondent's Services.

7.13.1 MSI Services Disaster Recovery Planning

DIR expects the Successful Respondent's DRP to provide sufficient level of detail for the Successful Respondent to successfully recover to support the Services as per the agreed Service Levels. The Successful Respondent shall comply in developing, maintaining and implementing a DRP to recover the Successful Respondent Shared Services Systems and upon the occurrence of a disaster, the Successful Respondent shall promptly implement its DRP to recover such systems. Successful Respondent shall develop for DIR's approval a DRP that includes the Successful Respondent's Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for each System. Successful Respondent shall maintain and test its own DRP.

The Successful Respondent shall, at a minimum:

7.13.1.1 Update, maintain, manage, test and implement any portion of the Successful Respondent Business Continuity and DRPs and activities that relate to the continued provision of the Successful Respondent's Services.

7.13.1.2 Ensure the DRP adheres to the Disaster Recovery Plan standards as defined in the SMM and will contain, at a minimum, details outlining all aspects of the plan, declaration criteria and recovery steps (e.g., IT Disaster Declaration Criteria, IT Call-Out Procedure, System Recovery Plan, Contingency Mode Resource Plan, Notification and Reporting, Return to Normal Operating Mod).

7.13.1.3 Ensure proper linkage between the Business Continuity Plan and DRP to make them holistic and integrated.

7.13.1.4 Provide DIR with Successful Respondent's criteria and procedures for declaring a disaster at a Successful Respondent facility or a Successful Respondent's Third Party

Exhibit 2.1 Statement of Work   Page 129

facility.

7.13.1.5 Provide a single point of contact for Business Continuity and Disaster Recovery plans, related communications and other activities that are Successful Respondent's responsibility.

7.13.1.6 Integrate the Disaster Recovery plan with the Business Continuity Plan related at a minimum to the following aspects:

   7.13.1.6.1 Emergency Response Plan.

   7.13.1.6.2 Damage Assessment Plan.

   7.13.1.6.3 Vital Records Plan.

   7.13.1.6.4 Crisis Management and Public Relations Plan.

   7.13.1.6.5 Security Plan.

   7.13.1.6.6 Personnel Plan.

   7.13.1.6.7 Communication Plan.

   7.13.1.6.8 Finance and Administration Plan.

7.13.2 MSI Services BCP and DR Testing

For the Successful Respondent provided Services, the Successful Respondent shall be responsible for the development and maintenance of Business Continuity Planning Testing Plans and Disaster Recovery Testing Plans, scheduling and project management of the testing, and identification, logging and resolution of issues resulting from the testing. Such tests will be scheduled in compliance with **Exhibit 2.3 IT Service Management Continuity**. The Successful Respondent shall, at a minimum:

7.13.2.1 Establish test objectives with DIR designed to verify that all Services supporting the DIR Shared Technology Services will be available within an established timeframe.

7.13.2.2 Coordinate acceptance of the test plan amongst DIR and Service Component Providers.

7.13.2.3 Perform annual table top execution of the Business Continuity Planning Testing Plans (BCP Testing).

7.13.2.4 Perform annual system failover execution of the Disaster Recovery Testing Plans (DRP Testing).

7.13.2.5 Schedule testing dates for BCP Testing and DR Testing with DIR and SCP(s) approval and give them the opportunity to observe and participate in the tests.

7.13.2.6 Test all components of the BCP Testing and DR Testing as required in cooperation with DIR and SCPs.

7.13.2.7 Assume coordination and administrative responsibility for Third Party Vendors utilized by MSI and during testing in accordance with the DRPs.

Exhibit 2.1 Statement of Work   Page 130

7.13.2.8 Continue to operate and manage the Services during periodic BCP Testing and DR Testing.

7.13.2.9 Provide DIR with a formal report of the test results within thirty (30) days of each test. At a minimum, these reports should include:

7.13.2.9.1 The results achieved.

7.13.2.9.2 A comparison of the results to the measures and goals identified in the respective plans.

7.13.2.9.3 A report on the feedback from DIR and SCPs as to the adequacy of continuity for their respective areas.

7.13.2.9.4 A plan and a schedule to remedy any gaps revealed during testing.

7.13.2.10   Through coordination with DIR and SCPs, ensure that Successful Respondent Services application integrity exists after restoration in accordance with the formal DRP.

7.13.2.11   Retest within ninety (90) days if any disaster simulation(s) fails to achieve specified results due to Successful Respondent's failure to perform its responsibilities.

7.13.2.12   Update the Disaster Recovery plans upon re-testing and verify that the remedy was successful.

7.13.3 MSI Services Disaster Recovery Execution

The Successful Respondent is responsible for activities required to recover the MSI's Services in the event a disaster is declared. The Successful Respondent shall, at a minimum:

7.13.3.1 In the event of a disaster, the Successful Respondent shall continue to be liable for performing their role unless it submits a waiver in writing.

7.13.3.2 Comply with DIR's definition and procedures for declaring a disaster.

7.13.3.3 Report disasters (or potential disasters) to DIR immediately upon identification based on parameters defined in the DRPs, and consult with DIR for an official declaration of a disaster as appropriate.

7.13.3.4 For all facilities or Services where Successful Respondent has sole oversight responsibility, declare disasters in accordance with procedures existing at the time of declaration and notify DIR of situations that may escalate to disasters as soon as practicable.

7.13.3.5 Execute the Disaster Recovery plans including:

7.13.3.5.1 Install or coordinate the installation of Equipment.

7.13.3.5.2 Operate the Equipment.

7.13.3.5.3 Restore the Software.

7.13.3.5.4 Verify that data is recovered to the appropriate point in time.

Exhibit 2.1 Statement of Work   Page 131

7.13.3.5.5 Provide all other functions associated with the Services.

7.13.3.5.6 Support SCPs as required to bring their affected systems and Services back into production mode.

7.13.3.5.7 In accordance with the Disaster Recovery plans, determine what resources to deploy.

7.13.3.5.8 Conduct, supervise, and administer the operation and implementation of such resources.

7.13.3.5.9 Provide additional resources as necessary to maintain provision of the Services for unaffected areas and re-align technical resources to maintain Business Continuity.

7.13.3.6 In accordance with the Disaster Recovery plans, assume coordination and administrative responsibility for Third Party Vendors utilized in the delivery of Services.

7.13.3.7 In accordance with the Disaster Recovery plans, develop a plan for the return of the Successful Respondent's Services to the original processing site or an alternate(s) site agreed to by DIR.

7.13.3.8 Provide for a return of readiness to respond to a Disaster, as set forth in the Disaster Recovery plans.

Exhibit 2.1 Statement of Work   Page 132